View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Calhoun, Institutional Archive of the Naval Postgraduate School

Calhoun: The NPS Institutional Archive

Theses and Dissertations | Thesis Collection

2006-03

Essential elements for preparedness planning

O'Brien, John E.

Monterey, California. Naval Postgraduate School

http://hdl.handle.net/10945/2959

http://www.nps.edu/library

Calhoun is a project of the Dudley Knox Library at NPS, furthering the precepts and goals of open government and government transparency. All information contained herein has been approved for release by the NPS Public Affairs Officer.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

ESSENTIAL ELEMENTS FOR PREPAREDNESS PLANNING

by

John E. O'Brien

March 2006

Thesis Advisor:	Robert L. Simeral
Second Reader:	Ted G. Lewis

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** March 2006	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Essential Elements for Preparedness Planning			**5. FUNDING NUMBERS**
6. AUTHOR(S) John E. O'Brien			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

The author of this thesis asserts that the unique nature of the modern threat environment removes all justifiable options for the providers and users of threat information to operate at arm's length from one another. If the two communities are not integrated to the point that collaboration can proceed unhindered, the flow of information between them will likely be sluggish, unidirectional and largely irrelevant. Collaboration involves more than just the flow of new information, however. It requires the exchanging of ideas, the challenging of assumptions and biases, and leads to the formation of a networked environment that is needed to defeat our networked adversaries. An organization that fails to accomplish this level of integration and collaboration runs the risk of finding itself preparing for yesterday's attack, and failing to prevent, prepare for or adequately respond to tomorrow's threat. The 9/11 Commission's synthesized protocol for scenario development and intelligence tasking is presented as a means of fixing this problem.

14. SUBJECT TERMS Intelligence, Vulnerability Assessment; Critical Infrastructure Protection; Collaboration; Nuclear Security; September 11; 9/11; Terrorism; Terrorists; Homeland Security; Counterterrorism			**15. NUMBER OF PAGES** 73
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

ESSENTIAL ELEMENTS FOR PREPAREDNESS PLANNING

John E. O'Brien
EK-4, United States Department of Energy
B.S., New Mexico State University, 1981
M.S., Johns Hopkins University, 1984

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
March 2006

Author: John E. O'Brien

Approved by: Robert L. Simeral, CAPT, USN (Ret)
Thesis Advisor

Ted G. Lewis, PhD.
Second Reader

Douglas Porch
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The author of this thesis asserts that the unique nature of the modern threat environment removes all justifiable options for the providers and users of threat information to operate at arm's length from one another. If the two communities are not integrated to the point that collaboration can proceed unhindered, the flow of information between them will likely be sluggish, unidirectional and largely irrelevant. Collaboration involves more than just the flow of new information, however. It requires the exchanging of ideas, the challenging of assumptions and biases, and leads to the formation of a networked environment that is needed to defeat our networked adversaries. An organization that fails to accomplish this level of integration and collaboration runs the risk of finding itself preparing for yesterday's attack, and failing to prevent, prepare for or adequately respond to tomorrow's threat. The 9/11 Commission's synthesized protocol for scenario development and intelligence tasking is presented as a means of fixing this problem.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

It is tempting to use the term “long and arduous” to describe this program of study. After all, it involved months of heavy mental lifting and many weeks of separation from my wonderful family (for whose love, patience and constant encouragement I am deeply grateful). But during those weeks and months, thousands of men and women served on the front lines in the fight for freedom, providing my family with the safety and security that enabled us to enjoy life, liberty and the pursuit of happiness with hardly a thought about our own safety. Those defenders, not I, are the ones who know what it means to be separated from family; they know what it is to wonder whether they would ever see their friends and loved ones again. They, not I, have earned the right to say *long and arduous*. How pitifully inadequate are mere thanks to people such as these!

When we consider those who have not yet returned, those who are returning with permanent impairment, and those whose families will never again enjoy their fellowship, the sentiment expressed by President Lincoln at Gettysburg becomes even more grand than Lincoln himself could have imagined; for these fought not only for the protection of their own nation, but so that countless others might taste the freedom which we so often take for granted.

> It is rather for us to be here dedicated to the great task remaining before us–that from these honored dead we take increased devotion to that cause for which they gave the last full measure of devotion–that we here highly resolve that these dead shall not have died in vain–that this nation, under God, shall have a new birth of freedom–and that government of the people, by the people, for the people, shall not perish from the earth.
>
> President Abraham Lincoln
>
> Gettysburg, Pennsylvania
>
> November 19, 1863

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

> A rededication to preparedness is perhaps the best way to honor the memories of those we lost that day.[1]

A. ENHANCING PREPAREDNESS

This thesis is about enhancing preparedness to reduce our nation's vulnerability to terrorist attacks. Specifically, the focus is on the process of creating and executing plans in a way that makes the best use of scarce resources for the goals of preventing attacks and protecting our citizens and critical infrastructure. Various planning methods will be examined as well as the way that each is challenged by today's threat environment.

B. CONTINUOUS IMPROVEMENT

The goal of these pages is to assist with the development of good terrorism preparedness plans, but perhaps most importantly, to present a mechanism for continuous improvement of those plans, an element that is often overlooked or is insufficiently robust, regardless of which planning mechanism is used. To use a plan for the sole purpose of setting initial conditions is fatal. Without a dynamic, continuously improving cycle of planning, we can never hope to stay ahead of a sophisticated adversary who knows how to use asymmetric techniques to leverage weakness into strength. This adversary is not satisfied with developing a plan and putting it on the shelf. Instead, he is always scanning the environment (our environment), probing for weaknesses, building plans that show promise and dropping those that do not as the environment changes; always seeking to avoid the fatal error of becoming fixated on a favorite plan and blinded to better ones. We must do no less.

If we are to succeed in this preparedness mission, we must understand the dangers that are unique to asymmetric conflict and how those dangers require us to change the way we plan and operate so that we can maximize our preparedness. Some of these threat characteristics will be presented in Chapter II, The Post-9/11 Threat Environment.

[1] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (New York: W. W. Norton & Company, 2004), 323.

Chapter III, Planning to Plan, will give a brief overview of how defense planning has changed since the end of the Cold War, and why the new threat environment has forced military and homeland security planners to develop new planning methodologies.

Chapter IV, Tempo: Using Time as a Tool of Strategy, will demonstrate that planning tempo can be just as important as combat tempo in gaining and maintaining one's advantage over an adversary.

Chapter V, It Takes a Network, will introduce some of the ways that modern terrorist organizations have adopted network characteristics and how those characteristics present us with unique challenges and opportunities. One of the lessons of network analysis is that we also must adopt certain network-like characteristics if we are to succeed in a struggle against a networked adversary.

New ways of collaborating, planning, tasking intelligence collection and disseminating intelligence information will be proposed in Chapter VI, A Model for the Future. The 9/11 Commission's four-step protocol for planning and intelligence collection will be presented, along with the essential element that must be included if their protocol is to succeed. The implications of the decision by Congress to cancel what might have been the only serious attempt by a government organization to implement the 9/11 Commission's protocol will also be considered.

To demonstrate the broad applicability of the principles in this document, the domestic nuclear weapon facilities owned by the United States Department of Energy (DOE) will be used as a case study in Chapter VII, Application to the Department of Energy. DOE has a robust planning strategy that avoids many of the pitfalls of other methods. But as the threat has grown since 9/11, DOE is understandably wrestling with new challenges to its dual commitments to be good stewards of the national stockpile of nuclear weapons and the taxpayers' money. DOE's planning methodology will be presented, along with an analysis of how it might be strengthened using the approach described in the following chapters.

Chapter VIII, Conclusion, will revisit the importance of preparedness and planning, and will examine the 9/11 Commission's "failure of imagination" criticism in light of the approach that is recommended in this thesis.

II. THE POST-9/11 THREAT ENVIRONMENT

> Iraq has become a point of attraction and restorer of (our) energies.
>
> – Osama bin Laden[2]

> The lesson of 9/11 for civilians and first responders can be stated simply: in the new age of terror, they—we—are the primary targets. The losses America suffered that day demonstrated both the gravity of the terrorist threat and the commensurate need to prepare ourselves to meet it.
>
> – The 9/11 Commission[3]

A. THE ONLY SUPERPOWER

In 1991, America's success in *Operation Desert Storm* served as a wake-up call to the world and helped lead us into a new, but significantly more dangerous era. As global news broadcasts showed live coverage of the unbelievable speed and efficiency with which the United States defeated one of the largest military forces on earth, there was no doubt that the world's only remaining superpower could not be seriously challenged, much less defeated, through conventional means. Our adversaries have begun using, and planning to use, non-conventional means in an effort to force us to respond to their political agenda. Homeland security practitioners must understand the nature and implications of this new threat environment.

B. THE POWER OF ASYMMETRIC CONFLICT

If someone had announced in the early hours of September 11, 2001 that they would destroy the World Trade Center towers in New York City with a few box cutters before the morning was over, it is hard to imagine that anyone would have taken them seriously. And yet that is what happened on that fateful morning. Such is the power of asymmetric conflict. The combatant who is skilled in asymmetric conflict finds the adversary's weakness and leverages it into overpowering strength. That weakness can be

[2] From transcript of a recording that was broadcast worldwide on January 16, 2006.

[3] *The 9/11 Commission Report*, 323.

physical, such as an insufficiently protected asset, or it can be cognitive, such as an insufficient understanding or an incorrect assumption. The attacks of 9/11 exploited both types of weakness.

After the end of the Cold War, and especially since 9/11, "[t]he threat environment *expanded* from a strategic, nuclear, symmetric threat from bombers, intercontinental ballistic missiles, and air- or sea-launched cruise missiles to a continuing symmetric threat, and an emergent asymmetric threat, which was focused across all domains, borders, and agencies."[4]

The above description is particularly useful since it reminds us that the threat environment has expanded, and not merely shifted from one type of threat to another. The threat of traditional, symmetric, nation-against-nation warfare might not seem imminent since 9/11, but it has never gone away.

In the old era of worrying predominantly about symmetric threats, our satellites and spy planes produced images that enabled analysts to count aircraft and troops, to find out which military and industrial assets were being moved or changed, and where new factories were being built. The domains and activities of our Cold War opponents were so sprawling and slow moving that we were able to maintain a reasonable flow of information about our adversary's strengths and intentions through technical means, informants and our own spies. Such is not the case in the new threat environment.

C. THE "LOW SIGNATURE" ADVERSARY

The most immediate threat to the homeland is the low-signature adversary. That is, the terrorist who blends in so well with the population he or she plans to attack, that there are few, if any, opportunities for the intended victim to get indications or warnings before an attack. Many of the terrorist's preparations would be considered legal and perfectly normal to an observer. Is the person who is photographing the Golden Gate Bridge a tourist or a terrorist? Is the person who is purchasing chemicals at the farm supply store planning to feed thousands or poison them? Intentions make all the

[4] Joseph R. Inge and Eric A. Findley, "North American Defense and Security after 9/11," *JFQ*, no. 40 (First quarter 2006): 24-25.

difference, yet intentions rarely announce themselves in advance, nor do they leave much of a paper trail. Today's terrorist is not simply willing, but often is planning to die in the process of carrying out an attack, a characteristic that is very much unlike traditional, symmetric threats. Terrorists are determined, innovative and able to carry out coordinated attacks against multiple targets. In some cases, the volunteer who will become the next suicide bomber might not be selected until the day of the bombing, making it virtually impossible to know in advance about planned terrorist operations.

Ambassador Henry Crumpton, the Department of State's Coordinator for Counterterrorism, describes this enemy as transformative, and the new battlefield as global and rapidly evolving. He told Congress that this new enemy is becoming increasingly lethal as they learn to deploy in smaller numbers, or perhaps even operate remotely. This enemy sees the war in Iraq as both a training center and an indoctrination center for extremists from around the world. This enemy wants not only to defeat the coalition that invaded Iraq, but they want to defeat the very idea of democracy in the Middle East.[5]

This adversary perfects his deadly skill by participating in, or at least learning from, the insurgency operations in Afghanistan and Iraq. In fact, those operations have been characterized as the most effective training ground for terrorists. Those who survive their insurgency operations have become skilled, combat-hardened veterans who may then train others and export their terror to other countries.

D. RETHINKING INTELLIGENCE

Ephraim Kam, reflecting on the phenomenon of surprise attacks, wrote, "History does not encourage potential victims of surprise attack. One can only hope to reduce the severity – to be only partly surprised, to issue clearer and more timely warnings, to gain a few days for better preparations – and to be more adequately prepared to minimize the

[5] Henry A. Crumpton, "U.S. Counterterrorism Strategy Update," in House International Relations Committee Subcommittee on International Terrorism and Nonproliferation held in Washington, D.C., October 27, 2005, U.S. House of Representatives. Available [online]: http://usinfo.state.gov/is/Archive/2005/Oct/28-580190.html. (accessed January 26, 2006).

damage once a surprise attack occurs."[6] In a similar vein, the respected analyst of the Pearl Harbor attack, Roberta Wohlstetter, wrote, "It would be reassuring to believe that Pearl Harbor was just a colossal and extraordinary blunder. What is disquieting is that it was a supremely ordinary blunder."[7]

History tells us that anticipating surprise attacks, even major attacks from a symmetric adversary who has thousands of aircraft, tanks and combatants, is difficult to do. Since there is so much evidence to substantiate the difficulty of this problem when faced with a large-scale attack, we should not be surprised that it is virtually impossible to get advance warning of a low-signature terrorist attack. Of what use, then, is intelligence information in this new era?

We must rethink how we use intelligence in the post-9/11 era. Although we should not give up trying to develop our intelligence capabilities and sources to the point that they can provide us with good indications and warnings, we must never presume that those resources will ever be able to tell us the day and hour of an impending attack beforehand. Instead, we must put most of our intelligence efforts and expectations into helping us understand our enemy, into helping us know how an attack is likely to occur so we can take measures now to harden targets against such attacks. We must also ensure that intelligence and threat information is disseminated as widely as possible so that many people can be working together to think of efficient ways to harden our critical infrastructure and protect our citizens.

---

[6] Ephraim Kam, *Surprise Attack: The Victim's Perspective* (Cambridge, MA: Harvard University Press, 1988), 233.

[7] Roberta Wohlstetter, *Pearl Harbor: Warning and Decision* (Stanford, CA: Stanford University Press, 1962), vii.

III. PLANNING TO PLAN

> The Allegan County Board of Commissioners has a plan. That plan is to develop a plan that will help them plan out their long-term strategic planning.8

A. CHALLENGES FOR DEFENSE AND SECURITY PLANNING

Any plan worth using is challenging to create. One reason good planning is hard to do is that planning involves contingencies that cannot be precisely defined, and it is hard to make a case for significant allocation of resources against "soft" contingencies. The need for a new method of defense planning became clear at the end of the Cold War, when the United States no longer needed to maintain a force structure that was designed primarily to fight a war against one or two nation-states. The system that has evolved since 2001 is applicable, with appropriate modifications, to homeland security.

B. THE RISE OF CAPABILITIES-BASED PLANNING

A system called Capabilities-Based Planning (CBP) was officially embraced by the DoD in its 2001 Quadrennial Defense Review.[9] CBP has been defined as "planning, under uncertainty, to provide capabilities suitable for a wide range of modern-day challenges and circumstances while working within an economic framework that necessitates choice."[10] This definition, has been adopted for use in Department of Homeland Security policy, and can be dissected into three basic elements: (1) uncertainty, (2) preparation for a wide range of challenges, and (3) an economic framework that necessitates choice. An examination of those elements reveals that CBP is not a radically new concept. Each of those elements has been present in earlier forms of defense planning, usually referred to as threat-based or scenario-based planning. The

---

8 Regan Foster, *Holland Sentinel*, July 2, 2004.

9 The timing of the QDR might lead one to the conclusion that it was a reaction to the terrorist attacks of 9/11. In fact, the QDR report was almost ready for final publication on 9/11, and was officially released less than three weeks later, on September 30, 2001.

10 Paul K. Davis, *Analytic Architecture for Capabilities-Based Planning, Mission-System Analysis and Transformation* (Washington, D.C.: RAND National Defense Research Institute, 2002), 1.

distinction lies in the emphasis placed upon the first two elements of the definition, namely, uncertainty and the wide range of challenges. The reasons for these new emphases are described below.

1. From Relative Certainty To Uncertainty

Defense planning during and immediately following the Cold War focused primarily on the few worst-case scenarios that could be directed at us by more-or-less symmetric adversaries. The prevailing view was that as long as our plans and capabilities were sufficient to defend against those worst-case threats or scenarios, then we could have a reasonable level of assurance that our capabilities would be adequate protection against lesser threats, even if those threats had not been envisioned by the planners.

The Cold War, Soviet-centric threat was risk-averse and had no interest in putting the doctrine of Mutually Assured Destruction to the test. We understood the Soviet Union and its plans for war reasonably well; well enough, at least, to have a reasonable expectation of getting some measure of warning of an impending attack. The terrorist threat, according to Paul K. Davis, is much worse. "Although the forces involved are small, they are in nearly all other respects more troublesome: They have positive incentives (even if bizarre by our reasoning) to use WMD, their tactics are unpredictable, and so on."[11]

2. From Relatively Limited, To Virtually Unlimited, Challenges

In the above quotation, Davis described the terrorists as having and using unpredictable incentives and tactics, even to the point of desiring to use weapons of mass destruction. On September 11, 2001, the North American Aerospace Defense forces were prepared for an invasion by foreign combat aircraft, but those forces were not prepared for a tactic as unpredictable as using domestic, commercial airliners as guided missiles. Terrorist leaders have made no secret about their desire, and their religious justifications and clerical authorizations, for using all possible means, including nuclear weapons, to destroy those who are not faithful to their radical brand of religion. Since many of those who threaten us are non-state actors, they have very little to lose. Even their own lives are of little value to them, compared to the benefits of paradise which they expect to receive as a result of their destructive actions. This kind of threat opens up an

[11] Davis, *Analytic Architecture for Capabilities-Based Planning*, 17-18.

entirely new and seemingly endless list of potential attack modes for which we must prepare and against which we must defend. The Departments of Defense and Homeland Security may not rely simply on defending against one threat group or one scenario.

As a result of this expansion of the threat, the focus of the Department of Defense has now moved into the realm of acquiring capabilities to enable the delivery of "effects" according to four standards:[12]

- Scale (size, intensity)
- Temporal aspects (latency, duration, time-phased application)
- Observability aspects (detection, attribution)
- Spatial aspects (distance, area)

This new capabilities-based focus is intended to provide flexibility to address known threats as well as those for which no explicit plans have been developed.

C. HOW MUCH IS ENOUGH? – PART I

Despite the rapid adoption of CBP in the Departments of Defense and Homeland Security, the process is not without its detractors. One particularly critical paper on the subject expressed concern that CBP, at least as it was initially planned for implementation by the Bush administration, would disconnect requirements from resources and make it very difficult for the military services to know when they have succeeded in doing enough.

> Pure capabilities-based planning would be like outfitting a toolbox with the latest, most desirable items for supporting the military strategy. But how big of a toolbox should you build? How many of each tool do you need? How many of these tools need external support in getting to the job at hand? How do you judge along the way if you are meeting defense objectives if there exists no metric against which to measure progress? Planning in such a vacuum does not allow an honest, accurate assessment of true military force requirements when no benchmark conflicts are offered. Military services attempting to support such a plan will find it

[12] Ryan Henry, "Defense Transformation and the 2005 Quadrennial Defense Review," *Parameters* 35, no. 4 (Winter 2005-06): 12.

> difficult to budget for unknown quantities of capabilities, potentially resulting in service rivalries that could easily drive resource requirements beyond reach.[13]

This author concluded that CBP, more so than older defense planning methodologies, is particularly unhelpful in defining how much capability is enough.

Davis helps to answer this question by pointing out that CBP needs to determine not only *what* needs to be done, but also *how quickly* it needs to be done.[14] Quickness, in this case, may be measured either in time or distance; for example, a requirement to halt an advancing adversary (the *what*) within 24 hours or within 50 miles (*how quickly*). A simple example helps illustrate Davis' point. If the healthcare industry in a fictitious nation were to use a centralized CBP approach, the planners might wonder how many ambulances the country would need. No one would argue that ambulances were an essential capability for the healthcare "toolbox," but they might argue about how many were needed. In this case, the primary metric for this decision would be the maximum number of minutes allowable from the time an ambulance is dispatched until it arrives on the scene. That metric would not be strongly dependent upon any particular scenario, other than allowing for normal traffic delays. A second metric would be an estimate of how many ambulances might need to be dispatched simultaneously from a given staging point, based upon population density in that particular area. This metric might be much more scenario-dependent, and would have to be carefully thought out based upon estimated likelihood of potential mass-casualty incidents such as natural disasters, large fires or accidents, or large-scale terrorist attacks. Defining how quickly effects must be delivered helps to answer what kinds of capabilities are needed, and how much of each kind. In other words, the required tempo of "effects delivery" – whether those effects are delivered by an ambulance crew or combat air support – helps answer the question of how much is enough. This question will be discussed further in Chapter 6, *A Model for the Future*. The next chapter will show that establishing and maintaining another kind of tempo in the months and years *before* an attack is just as important to preparedness as is the tempo of effects delivery during the response and recovery phases.

---

[13] Jeffrey B. Kendall, *Capabilities-Based Planning: The Myth* (National Defense University, National War College, 2002), 5.

[14] Davis, *Analytic Architecture for Capabilities-Based Planning*, xxii, 32.

IV. TEMPO – USING TIME AS A TOOL OF STRATEGY

> This day ordinary Americans took extraordinary steps to help their fellow Americans and by doing so gave the greatest sacrifice.[15]

A. THE MOST IMPORTANT CAPABILITY

Effective planning for preparedness in today's threat environment must be treated as an essential capability. In their draft National Preparedness Goal, DHS has stressed the importance of planning with these words: "Planning is the foundation on which all other capabilities are developed and enhanced, and is essential to their successful achievement."[16] Planning for homeland defense and homeland security should be thought of as a technological capability that must be developed and kept current. We must never assume that today's planning technology will be adequate for tomorrow's threats.

The previous chapter described the shift from threat- and scenario-based planning to the capabilities based planning approach now being used by the Departments of Defense and Homeland Security. Critical Infrastructure Protection (CIP) analysts must be mindful of more than just their planning methodology, however. They also must be aware of their planning tempo. Military planners are familiar with the concepts associated with the tempo of combat; concepts which include things such as the intensity of combat, the frequency and duration of effects delivery, the rate of resupply – in general, the overall intensity and rate at which events unfold during combat. Combat tempo is designed to put the enemy off balance and keep him always in a reactive mode. Cold War planners were relatively safe in maintaining a steady and more or less symmetric planning tempo on both sides of the conflict. It was much easier for Cold War opponents to keep an eye on each other, knowing that any worrisome upgrade to military capabilities would take years to accomplish and would be accompanied by many

---

[15] From Angels of Freedom plaque, Flight 93 Crash Site, Shanksville, PA.

[16] Department of Homeland Security, *Final Draft of National Preparedness Goal* (Washington, D.C.: Department of Homeland Security, December, 2005), 87.

opportunities to discern the opponent's intentions. Today's planners must move beyond the outdated notion of a slow-moving and slow-planning adversary if they are to avoid a tempo deficit that would give an asymmetric advantage to would-be terrorists.

B. PRELUDE TO ACTION: COLONEL BOYD'S 'OODA LOOP'

Air Force Colonel John Boyd (1937-1997) developed a useful means of looking at the cycle of planning and action. He and his colleagues prepared a diagram that is designed to help understand the mental processes of observation, orientation, decision and action that fighter pilots unconsciously go through multiple times per second during aerial combat. His Observe – Orient – Decide – Act diagram, or "OODA Loop" is shown in Figure 1. The OODA Loop concept has been applied to processes as diverse as combat training and business competition. The straightforward nature of the Observe – Orient – Decide – Act nomenclature belies the subtlety and power of Colonel Boyd's conception, however.

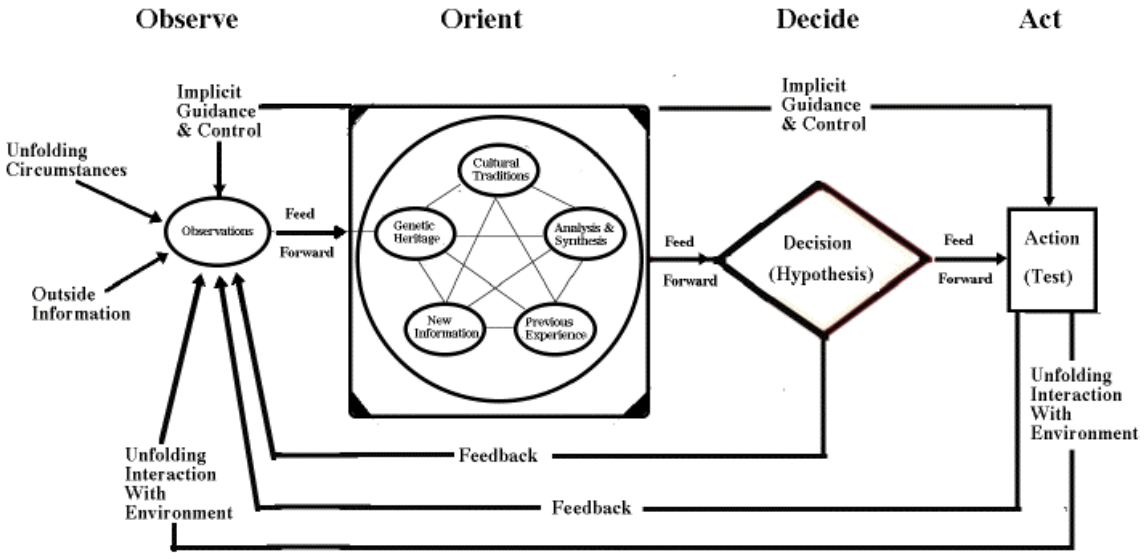

Figure 1. Colonel John Boyd's OODA Loop
Source: http://en.wikipedia.org/wiki/OODA_loop

The reason for the popularity and broad application of Colonel Boyd's idea is not merely its somewhat intuitive progression from observation to orientation, decision and action, but because of the notion that success is achieved by being able to cycle through one's OODA loop faster and more effectively than one's adversary or competitor. Colonel Boyd believed that if a combatant could observe his adversary's actions with sufficient frequency and clarity, with constant feedback about the adversary's maneuvers and counter-maneuvers, he would begin to get an intuitive sense that would help him anticipate his opponent's next move. The pilot who could achieve this intuitive sense during aerial combat would have an enormous advantage, even if his adversary happened to be flying a superior aircraft. This is not an attempt to achieve some sort of mystical clairvoyance, but rather to acquire, gather and understand information at a rate sufficient to know how this particular adversary operates. This idea is sometimes referred to as "operating inside the enemy's (competitor's) OODA loop." Boyd's biographer wrote that understanding this process enables a commander to compress the time between observation and action, and to use this advantage to confuse the enemy by acting in an unexpected manner. These two factors – time compression and unexpected action – can cause confusion and an inefficient use of time by the adversary.[17]

Boyd believed that some kind of OODA Loop advantage accounted for the ten-to-one kill ratio advantage that American F-86 pilots maintained over their MiG-15 pilot counterparts during the Korean war, even though the American pilots had not been trained in advanced OODA Loop techniques. The MiG-15 was an aerodynamically superior aircraft, yet Boyd concluded that two characteristics of the F-86 made its superior combat performance possible. First, the design of the F-86 cockpit canopy provided a greater field of view than did the MiG-15 canopy. This canopy gave the American pilots more opportunity to accurately observe and orient himself during combat maneuvers, and therefore a greater opportunity to decide and act more effectively and rapidly so as to confuse and outmaneuver the enemy pilot. Second, the hydraulic controls

[17] Robert Coram, *Boyd: The Fighter Pilot Who Changed the Art of War* (Boston: Little, Brown & Company, 2002), 336.

in the F-86 allowed the American pilots to maneuver faster and more often than the pilots of the MiG-15 who would become fatigued trying to keep up using flight controls that took more physical energy to operate.

This powerful concept of "operating inside the enemy's OODA loop" is applicable to homeland security and counterterrorism planning in at least two ways. As its name implies, the "Observe" function in the OODA loop reveals the necessity of maintaining awareness of one's environment. In a homeland security setting, this means that CIP planners must have a steady stream of detailed information about demonstrated terrorist tactics as well as intelligence about possible terrorist plans. Even if the intelligence about the terrorists' plans is of undetermined credibility, it still provides the analyst with an increasing sense of what could happen in the future. The second way in which the OODA loop applies to counterterrorism planning can be seen by observing the "Orient" portion of the diagram. Orientation is the filter through which all facts and events are processed. If a CIP analyst is viewing the unfolding environment through a faulty orientation filter that hinders accurate assessments of the threat, then the analyst must engage in robust collaboration with others as well as consume a steady stream of new information to help overcome that bias. The more times an analyst can cycle through the OODA loop – observing the threat situation, orienting to new information, testing biases and theories, reorienting and observing again – the more likely that analyst will be able to get an intuitive feel for the way the adversary thinks and plans. This deep understanding of the adversary will help the analyst anticipate innovative attack scenarios and then develop the means to defend against those scenarios so as to protect the people and places he or she is charged to protect.

C. A TRAGIC ILLUSTRATION

One of the clearest illustrations of the OODA Loop principle occurred on September 11, 2001. The passengers of each of the four hijacked flights were aware for many minutes that their aircraft had been hijacked. Using the terminology of Boyd's diagram, the passengers had abundant opportunity to observe new information about "unfolding circumstances" and were undoubtedly trying to figure out how to properly orient themselves and their actions to that information. In particular, they were using

their experience and analysis/synthesis skills (see inside the "Orient" box in Figure 1) to help them decide what to do. Their experience told them that hijackings had always been used as a tool to force a government to negotiate with the hijackers, that hijackers were not likely to be suicidal, and the passengers would be released after the hijackers were reasonably sure their demands would be met. Our hindsight tells us that on 9/11, experience was a faulty guide for knowing what to do during a hijacking. The hijackers reinforced this misunderstanding by telling the passengers that everything would be fine if they just complied with orders. The hijackers were shrewdly exploiting an asymmetric advantage of information, and had, in essence, hijacked the passengers' ability to properly orient to what was really happening. Tragically, the deception was successful on three of the hijacked aircraft. By 9:37 a.m., two planes had crashed into the World Trade Center towers and one into the Pentagon. That is when things began to change on United Flight 93, originally bound for San Francisco, but later diverted toward our nation's capitol. As telephone conversations between Flight 93 passengers and observers on the ground began to bring fresh information about unfolding circumstances, the passengers were gaining better "visibility" of what was really going on. This new information enabled them to overcome the incorrect biases caused by their accurate recollections of previous hijackings. The passengers' newly corrected orientation allowed them to adjust their decisions and their actions. They began a counterattack against the hijackers in the cockpit at 9:57 a.m., approximately 29 minutes after the hijacking began. The hijackers, realizing they could not make it to their intended destination, crashed the plane into an open field near Shanksville, Pennsylvania at 10:02 a.m. The passengers' adjusted orientation and corresponding actions enabled them to bravely protect the lives of an unknown number of people who would have died minutes later in Washington, D.C.

Meanwhile, "orientation filters" were being recalibrated at FAA headquarters as well. For more than two years, since August, 1999, the FAA intelligence office had thought about the possibility of a suicide hijacking but considered it unlikely. On this misunderstanding, the 9/11 Commission wrote:

> The FAA analysts judged [a suicide hijacking] unlikely, because 'it does not offer an opportunity for dialogue to achieve the key goal of obtaining Rahman and other key captive extremists. ... A suicide hijacking is assessed to be an option of last resort.' Analysts could have shed some light on what kind of 'opportunity for dialogue' al Qaeda desired. The CIA did not write any analytical assessments of possible hijacking scenarios.[18]

The FAA analysts had assumed, based upon their accurate recollections of past hijackings, that any hijacking by terrorists would be for the purpose of negotiation (for Sheik Rahman's release from prison, for example). If those analysts had been aware of, and heeded, the CIA's intelligence reporting, they would have known that al Qaeda was more interested in killing Americans than in negotiating with them. This fact is painfully obvious to us now, but it was less so before 9/11. A clear understanding of al Qaeda's intentions might have motivated the FAA to increase aviation security as a deterrence measure against all hijackings, regardless of the motivation behind the hijackings.

The testimony of Richard Clarke before the 9/11 Commission reveals why the facts that are so obvious to us now were not so obvious before September 11, 2001. Mr. Clarke, the National Counterterrorism Coordinator from 1997 through 2001, told the Commission that the warning about the possibility of a suicide hijacking would have been just one more speculative theory among many, hard to spot since the volume of warnings of "al Qaeda threats and other terrorist threats, was in the tens of thousands – probably hundreds of thousands."[19] Mr. Clarke's statement suggests that too few people had access to enough of the facts to enable a process of sorting through the "speculative theories" and prioritizing them for actions as simple as hardening cockpit doors.

The events of 9/11 demonstrate the value of information sharing for CIP analysts; specifically the value of sharing information about new tactics being used by terrorists and insurgents as well as information about what the terrorists might be thinking about doing in the future. The information must be sufficiently fresh and unprocessed to contain the subtleties analysts need if they are to understand and overcome their own

[18] *The 9/11 Commission Report*, 345.

[19] *The 9/11 Commission Report*, 345.

biases, continuously test their own theories and adjust them as needed. Collaboration with other CIP analysts and with experts in areas such as intelligence will help identify biases and blind spots.

Homeland security planners are defending against a sophisticated foe. The daily news from Afghanistan and Iraq continues to reveal the insurgent's effective use of agile planning, effective observation, and skilled refinement of tactics. CIP analysts put themselves at a disadvantage when they try to respond to a high-speed, well-informed adversary with sluggish planning and outdated presumptions that remain unchallenged. Allowing one's enemy to gain an asymmetric advantage in the areas of information, planning and preparedness is to increase the probability of being surprised by – and unprepared for – the next attack.

THIS PAGE INTENTIONALLY LEFT BLANK

V. IT TAKES A NETWORK

> Whoever masters the network form first and best will gain major advantages.[20]

A. TERRORIST NETWORKS

The most basic definition of a network is a collection of nodes and links that connect pairs of nodes.[21] Nodes can be almost anything, from people or computers to cities or railway terminals. The variety of links can be just as diverse, including such things as transmission lines, roadways and railroad tracks.

The radical Islamist terrorist coalition has been described, studied and analyzed as a network. Marc Sageman describes how network analysis can be used to design a strategy for dealing with terrorists. He uses the technical term "scale free network" to describe the particular characteristics of the jihadist organization, and then points out the strengths, weaknesses and potential strategies associated with this type of network:

> This type of network is robust and resists random attack. Stopping terrorists randomly at our borders will not affect its structure. It may stop terrorists from coming here, but will leave the network undisturbed. However, it is vulnerable to targeted attack, namely against its hubs. If the hubs are destroyed, the system breaks down into isolated nodes. The jihad will be incapable of mounting sophisticated large scale operations like the 9/11 attacks and be reduced to small attacks by singletons. It is of course possible for such nodes to try to become hubs and create their own little networks. Ahmed Ressam tried to recruit new untrained collaborators in the Millennial Plot after his original co-conspirators were unable to travel to Canada. But such operations have not generally been successful. The hubs are vulnerable because most communications go through them. By following communications back to them, good police work would be able to identify and arrest these human hubs. This strategy has already shown considerable success.[22]

---

[20] John Arquila, David Ronfeldt, and Michele Zanini, "Networks, Netwar and Information-Age Terrorism," in *Countering the New Terrorism*, ed. RAND National Defense Research Institute (Washington, D.C.: RAND, 1999), 55.

[21] Ted G. Lewis, "Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation" (unpublished manuscript, Naval Postgraduate School, Monterey, California, 2004).

[22] From a presentation entitled "Global Salafi Jihad" given by Dr. Marc Sageman to the Department of Energy, Pantex Plant, Amarillo, TX, May 17, 2004.

This description of the jihadist network begins to suggest that our strategies to defend against it and defeat it require a new kind of thinking and planning.

B. RESILIENCY OF NETWORKS

Dr. Sageman's description of the global terrorist network, of which al Qaeda is only a small part, indicates that individual terrorists may be removed without seriously harming the overall network. He also points out that scale free networks are vulnerable to attacks against their hubs. Hubs are nodes – people in this case – who are more highly connected than most other people in the network. These nodes represent the terrorist leaders. Sageman suggests that if terrorist leaders are eliminated, this will have the effect of breaking the overall network down into a set of smaller subnetworks which would be unlikely to have the resources to coordinate and execute major terrorist attacks. It is possible that the Global War on Terrorism led by the United States has had this effect on al Qaeda, at least temporarily, and that is why there have been no major attacks against our homeland since 9/11. The insurgencies in Afghanistan and Iraq have shown, however, that numerous smaller attacks may be sustained in spite of the disruption caused by the loss of key terrorist leaders.

Networks, by nature, are strongly decentralized. In a twist of irony, al Qaeda's strong commitment to operations security might have harmed their ability to coordinate large attacks. Sageman suggests that al Qaeda's penchant for security causes them to act more like a hierarchy than a network in some ways. In particular, their tight security procedures force them to rely too heavily on their vertical, leader-to-subordinate, communication links. Such heavy dependence upon those links makes them more vulnerable to discovery, interception and destruction, and it prevents the extended network from having enough links to achieve maximum success in field operations. In fact, Sageman goes so far as to say that the field successes that al Qaeda has achieved was largely due to individual terrorists violating their own rules of tradecraft.[23] If this is true, it would be worth further study to see whether eliminating leadership "hubs" from a hybrid hierarchy/network has the unexpected effect of increasing the effectiveness of the remaining terrorists by forcing them to operate in a more agile, network-like manner.

[23] Sageman, "Global Salafi Jihad" presentation.

C. NETWORK VS. NETWORK

Network analysts who apply their techniques to the study of terrorist organizations often say that it takes a network to fight a network because a hierarchical command structure is at a disadvantage when trying to oppose a networked structure.[24] The reason for this is that the nodes (people) in a networked organization are much more highly connected to other nodes than are those in a typical hierarchical structure. Using the terminology from Boyd's OODA diagram in chapter 4, we would say that the people in a networked organization have better situational awareness, or more opportunity to "observe," because they have more links from which to gather new information, and the information they get is disseminated more rapidly. They are correspondingly better able to "orient" to the new information because of the greater opportunities for collaboration and interaction with people with diverse expertise and experience. All of these features give the networked organization the ability to plan, communicate and move resources much more quickly than they would if all information and resources were passed to, then distributed piecemeal from, a distant centralized command headquarters. Arquila, et al., cite criminal organizations, Colombian drug cartels, persistent religious movements in Algeria and the Zapatista movement in Mexico as examples of the ability of relatively small networked organizations to continually frustrate the larger hierarchical government structures that attempt to suppress or eliminate them. They suggest that governments must adopt the same network design principles as their adversaries, particularly a "willingness to innovate organizationally and doctrinally, and by building new mechanisms for interagency and multijurisdictional cooperation."[25]

D. ADVANTAGES OF A NETWORK

When it comes to planning for preparedness, a networked organization has several advantages over a hierarchical, bureaucratic organization. The following paragraphs describe some of those advantage-producing characteristics and why they are useful in today's CIP organizations.

---

[24] Lewis, "Critical Infrastructure Protection in Homeland Security"

[25] Arquila, et al., *Countering the New Terrorism*, 55.

1. Interconnectedness

Interconnectedness, in this context, is an expression of the need to maximize the number of sources of relevant information. The need for relevance might mean that some sources should be discontinued or monitored only infrequently, and that other sources should be cultivated. Interconnectedness is another way of saying "network" except with a greater emphasis upon the flow of ideas and information between participants. Interconnectedness implies that participants have ready access to much more information than that available from just their bosses and immediate co-workers. This access to information is necessary, even if the participants are in a hierarchical organization from a chain-of-command perspective. Interconnectedness is the organizational "highway" upon which collaborative interactions may travel. Without it, collaboration is severely weakened, or rendered impossible.

2. Timeliness Of Information

It should go without saying, yet we dare not leave it unsaid, that timeliness of information is essential to success. Timeliness of information is an essential characteristic for any organization that seeks to "operate inside the enemy's OODA loop." For the passengers of Flight 93 on 9/11, a delay of just a few minutes in receiving the bias-correcting information about the hijackings and crashes of the other three flights would have been too late. It is true that in the case of intelligence analysis, there is a tradeoff between accuracy and timeliness. The accuracy of an intelligence report might increase if the analyst is given more time to assimilate and verify information from multiple sources. Critical infrastructure protection analysts must help intelligence analysts know the appropriate balance between accuracy and timeliness. Miller put it well when he said, "Accuracy is a relative term, though. If increasing the accuracy of a product causes excessive delays in getting the information to the user, it simply becomes highly accurate, but unusable, 'news.'"[26] The 9/11 Commission's final report showed clearly that too much delay in gathering and connecting all the intelligence "dots" turned what might have been an opportunity for prevention into a major news event.

[26] Mark E. Miller, *The Integration of Operations and Intelligence: Getting Information to the Warfighter* (Air Command and Staff College, Research Department, 1997), 11, AU/ACSC/0362/97-03.

3. Information Sharing Environment

The 9/11 Commission devoted so much space in their final report to the institutionalized withholding of information inside government agencies that the result should have been to embarrass governmental institutions into fixing the problem as quickly as possible. But it takes work to make information sharing happen, especially when the old model of information ownership fits in so much better with established modes of agency and employee recognition.

The current administration has taken some steps to create a culture of information sharing. For example, through the Executive Order entitled *Further Strengthening the Sharing of Terrorism Information to Protect Americans*, the President of the United States has ordered federal agencies to enhance information sharing through such actions as:[27]

- giving the highest priority to, among other things, the interchange of terrorism information among agencies (including State, local, tribal and private),
- promptly giving access to the terrorism information to the head of each other agency that has counterterrorism functions,
- cooperating and facilitating production of reports based on terrorism information, and
- preparing terrorism information for maximum distribution (emphasis added).

The President's direction addresses interconnectedness by including a diverse group of agencies (state, local, etc.) and by requiring "maximum distribution" of terrorism information. Such direction from the President of the United States will, over time, ease the ability of organizations to establish linkages with other organizations. This was a necessary step of high-level policy, but it is not a sufficient step for ensuring adequate information sharing in the near term. The momentum must be generated and sustained through lower level policies and procedures that receive continuous encouragement and oversight by the President and Congress.

[27] U.S. President. *Executive Order*. "Further Strengthening the Sharing of Terrorism Information to Protect Americans." (27 October 2005). Available [Online]: http://www.whitehouse.gov/news/releases/2005/10/print/20051025-5.html. (accessed February 3, 2006).

Other enablers of information withholding are more subtle. The final report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction ("WMD Commission") revealed some surprising ways that information sharing can be subconsciously hindered by our rules on classification and handling of sensitive information. For example, some documents are stamped with the caveat, ORCON, meaning "originator controlled." The WMD Commission said this caveat gives the wrong impression that the collectors of intelligence "own" the information and should control access to it. The WMD Commission's report to the President also cited an historical imbalance between protecting sources and methods and the appropriate dissemination and sharing of information. They called for all intelligence information to be submitted by the collectors into an "Information Sharing Environment" that would balance protection and dissemination.[28] These observations by the WMD Commission are informative, but they will not, by themselves, generate the necessary changes in executive agencies without constant Presidential attention.

4. Integration vs. Synchronization

Since 9/11, much has been said about the need to "connect the dots," referring to the need to get all the disparate pieces of intelligence and other information into one place where analysts can begin to put them together into an overall picture. Perhaps the dots that are in most need of being connected are the ones within and between the myriad governmental organizational charts. For example, the diverse elements of operations and intelligence are often seen as two areas that need to be synchronized for maximum effectiveness; that is, intelligence information would be asked for and provided at just the right time to support the operation. But synchronization is not the same as collaboration. One can envision the operations expert and the intelligence analyst each staying within the bounds of their own organizations and exchanging just enough information for the operation to succeed. Mark Miller says that rather than synchronizing them, "we should be making strides to integrate the two disciplines. ... This mentality encourages development of a team that will strive to accomplish a common goal."[29] Miller's expression of integration is very close to collaboration. He continues:

[28] The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, *Report to the President of the United States* (Washington, D.C., 2005), 443-444.

[29] Miller, *The Integration of Operations and Intelligence,* 2.

> It is not enough for the intelligence community to improve its support to military operations; the operations community must do its part to communicate focused requirements that must be satisfied within the intelligence cycle. This can only be accomplished by understanding the capabilities of the intelligence community as well as the limitations. Operators must make a dedicated effort to include their Intel counterparts in all aspects of planning and execution and stop the process of using Intel to "fill gaps" in the plan. The frequently observed "just tell me what I need to know" attitude must disappear. Only then will Ops and Intel be integrated into a truly efficient team.[30]
>
> Intelligence simply must situate itself within the operational cycle rather than outside it. In other words, the intelligence collection, production, and dissemination cycle must be compressed so that it fits within the operational cycle for targeting to support strike and restrike operations."[31]

Miller promotes integration in his thesis, but the benefits he is describing are the fruits of something even greater than integration, and that is collaboration, a subject that will be discussed more thoroughly in the next chapter. Miller's promotion of integration seems to be based on the assumption that integration necessarily leads to collaboration. In the dynamic world of combat operations, this assumption is very likely to be valid. Where the pace is markedly more deliberate, however, as it is in strategic planning environments, a lack of collaboration would not be as immediately obvious, and integration alone might be insufficient. In homeland security planning environments however, a call for integration might lead to the misunderstanding that only two organizations are involved (intelligence and operations, for example), and that embedding one of them into the other would fix everything. Homeland security planning involves a multitude of organizations at the federal, state and local levels of government, and collaboration must be possible even where integration is not possible.

[30] Miller, *The Integration of Operations and Intelligence*, 3

[31] Ibid., 12.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. A MODEL FOR PREPAREDNESS

> Surprise ... includes gaps in intelligence, but also intelligence that, like a string of pearls too precious to wear, is too sensitive to give to those who need it.[32]

The previous chapters presented the case that the unique nature of today's threat environment must cause CIP organizations to carefully and deliberately design their approaches to such things as planning methodology, planning tempo and willingness to adopt network-like characteristics. This chapter will introduce the 9/11 Commission's recommended approach to planning and intelligence collection, and will present the case that effective collaboration is needed to pull these other elements together in a coherent and effective way.

A. COLLABORATION: THE ESSENTIAL ELEMENT OF PREPAREDNESS

The concept of collaboration has been mentioned several times in the preceding pages, and this section will expand upon the definition and benefits of collaboration. William Pelfrey reports that collaboration has been called "*the most essential element in the cycle of preparedness.*"[33] The following example of pre-9/11 interactions at the highest level of government will prepare the way for an examination of this bold assertion that collaboration is *the most essential* element in the context of preparedness.

Just one week before the 9/11 terrorist attacks, National Counterterrorism Coordinator, Richard Clarke, wrote a memo to the National Security Advisor in which he presented the view that al Qaeda was a nuisance that killed a few Americans every 18 to 24 months. Another school of thought viewed al Qaeda as the "point of the spear of radical Islam." The 9/11 Commission criticized the government for not forcing this argument into the open and letting those with diverse opinions enter into a debate on this subject.[34] Instead, each person or small group held their opinions in a vacuum, and the debate about the extent of the al Qaeda threat did not rise to a level that would have

[32] Wohlstetter, *Pearl Harbor*, viii.

[33] William V. Pelfrey, "The Cycle of Preparedness: Establishing a Framework to Prepare for Terrorist Threats," *Journal of Homeland Security and Emergency Management* 2, no. 1 (2005): 8.

[34] *The 9/11 Commission Report*, 343.

required further exploration or action. The 9/11 Commission report goes into further detail about the White House meetings and memos on the subject of the threat posed by al Qaeda. Were these people collaborating? The fact that people are meeting together does not necessarily indicate that collaboration is occurring.

To realize that the word is a combination of "co-" (meaning with or together) and "labor" is to begin to get at the heart of the power of collaboration. Those who are collaborators are not so simply because they have been directed to be in the same room or on the same conference call with one another. Collaboration goes beyond mere physical or virtual proximity. True collaborators are "co-laborers" with each other in practice, not just in name. This idea of laboring together conveys a unity of purpose and an equality of rank, at least in the sense of an equal ability to be heard and recognized during debate. James Surowiecki's book, *The Wisdom of Crowds*, offers several compelling examples of the value of collaboration within groups, as well as the tragic consequences that can occur when groups merely meet together but fail to collaborate. The vital element that seems to determine whether collaboration is real or imagined is an effective means of extracting and aggregating the information of everyone in the group. Surowiecki claims that the intelligence community's inability or unwillingness to aggregate the information and judgments of everyone who could have had some input to the pre-9/11 discussions was a vital failure in preventing the 9/11 attacks.[35]

1. The Crucible of Collaboration

If we juxtapose the preceding discussion about collaboration alongside the "Orientation" phase of John Boyd's OODA Loop (Figure 1), we find that this alignment highlights one of the greatest benefits of a strongly collaborative environment, and that is the opportunity for peers to hold each other accountable for their biases. Biases are inevitable, but they are dangerous when they are unrecognized, denied or unchallenged. As new ideas and information are brought into view, biases must be self-challenged and group-challenged. All participants must be willing to discard biases that cannot withstand this crucible of collaboration.

[35] James Surowiecki, *The Wisdom of Crowds* (New York: Anchor Books, 2005), 78.

One of the greatest hindrances to collaboration within and among government agencies is the bureaucratic friction that makes effective collaboration difficult or impossible. Like the energy-draining controls of the MiG-15 aircraft mentioned in Chapter 4, bureaucratic friction can drain the energy of those who want to innovate and collaborate, but find the friction simply too powerful to overcome. More often than not, bureaucratic friction is assumed to be a necessary evil of government bureaucracies. The nearly universal understanding of the equivalent term, "red tape," reveals the presumed inevitability of such friction. A close examination of each bit of friction-producing red tape reveals the almost universally benevolent rationale that, perhaps generations ago, intended to provide protection against wasteful spending or violations of civil rights. Without tearing down essential protections, CIP and intelligence organizations must remove all hindrances to effective information sharing and collaboration. Any attempt to protect the homeland without demanding and ensuring effective collaboration within and among all appropriate agencies is to guarantee our unpreparedness for future attacks. It is with good reason that collaboration – actual co-laboring – has been described as the most essential element in the cycle of preparedness.

B. WHERE THERE IS NO VISION, THE PEOPLE PERISH[36]

There must be something deep within the human heart that ensures our immunity and reflexive resistance to being ordered to do the very things we most need to do to survive. For example, statistics and our own casual observations reveal just how effective are the frequent exhortations for us as a nation to eat properly and exercise regularly. Similarly, a mandate for something as important as collaboration within the homeland security community might cause meetings to happen and money to be spent, but it will not result in *real* collaboration, at least not as it is described in these pages. To try to force collaboration rather than engendering a vision for it is to harden the victims of the mandate against the very idea, evoking the familiar bureaucratic mantra that "someday, this too shall pass." Recognizing this aspect of human nature is the first step in addressing the problem. Collaboration should be treated as a vision that must be caught. We must be imaginative in creating the need and desire for collaboration.

[36] Proverbs 29:18 (King James Version)

The 9/11 Commission wrote that even before 9/11 various government agencies had considered the idea of terrorists using hijacked aircraft as guided missiles, but each one discarded it from further consideration. The Commission added, "The challenge was to flesh out and test those scenarios, then figure out a way to turn a scenario into constructive action."[37] The notion of "fleshing out and testing scenarios" begs for a collaborative planning environment. The idea of establishing such an environment, and using it in the manner recommended in the literature developed in the years following Pearl Harbor, seems to be the crucial piece that was missing from pre-9/11 counterterrorism planning. It is imperative that every person responsible for counterterrorism – whether elected official, head of an agency or entry-level analyst – must catch this part of the 9/11 Commission's vision and push it forward as fast and as far as possible. The remainder of this chapter is designed to present the details of the 9/11 Commission's strategy and combine it with the elements from the preceding chapters (planning methodology, planning tempo, and the characteristics of networks, including collaboration) to provide a framework for CIP planners to advance the effectiveness of their own processes.

1. The Intelligence Cycle

The process by which the consumers of intelligence information submit their requests for new information, and how that information is collected, processed and disseminated is referred to as The Intelligence Cycle. One way of illustrating this process is shown in Figure 2, below.

As with so many other concepts in the field of protection planning, the metaphor of a cycle is useful. A cyclical process implies that there is no final end state; that the job is never finished completely. In fact, when it comes to preparedness planning, going through the cycle effectively *is* the job. The goal is to expand the two-dimensional cycle into a three-dimensional spiral, where the third dimension represents increasing effectiveness. A spiral shows continuous improvement, whereas a cycle that is confined to two dimensions represents going in circles, always doing the same thing, with hardly a thought about how to make things better.

[37] *The 9/11 Commission Report*, 346.

Figure 2. Typical Presentation of the Intelligence Cycle

Intelligence expert Mark Lowenthal knows from firsthand experience that the level of communication between collector and consumer implied by the diagram of the intelligence cycle is often not an accurate reflection of the real situation.[38] The intelligence community often produces new reports based upon old requests and entrenched reporting patterns, even when no one is asking for the specific information contained in the latest reports. This is an example of going in circles, rather ascending the spiral of increasingly effective tasking, collection and reporting. The intelligence community needs feedback from the consumers of the intelligence information so that collection and processing resources may be directed to the areas where they are most needed.

2. The Essential Vision

The 9/11 Commission had much to say about the process of intelligence collection tasking and reporting. In its final report, the Commission described the intelligence community's significant effort to study the phenomenon of surprise attack after the Japanese attack on Pearl Harbor. The various reports that emerged from this

[38] Mark M. Lowenthal, *Intelligence: From Secrets to Policy* (Washington, D.C.: CQ Press, 2003), 50-51.

research presented recommendations in a variety of ways, but the 9/11 Commission observed that they tended to have four elements in common. The Commission also asserted that if the intelligence community had tried to implement these four steps, the attacks of 9/11 might have been avoided. The four elements, as they were presented in the 9/11 Commission's final report, are:[39]

1. Think about how surprise attacks might be launched.
2. Identify telltale indicators connected to the most dangerous possibilities.
3. Where feasible, collect intelligence on these indicators.
4. Adopt defenses to deflect the most dangerous possibilities or at least trigger an earlier warning.

A cursory examination of these elements reveals that the third step is the entry point into the traditional intelligence cycle shown in Figure 2. The first two steps, therefore, should be *directed by the consumer* to focus intelligence collection to look for potential attack preparations. In other words, the consumer should not be merely a passive observer of the stream of reports that come from the intelligence community, but must be an active participant in directing the collection of new intelligence.

The only problem with the Commission's four step planning protocol is that its potential benefit can be neutralized by attempting to implement it in a hierarchical, stove-piped fashion rather than in a collaborative, networked fashion. Each step should be implemented in a highly collaborative environment using a group of people with a broad range of expertise and backgrounds.

3. Step 1: "Think About How Surprise Attacks Might Be Launched"

Security experts come face-to-face with a dilemma when they contemplate this component of the 9/11 Commission's recommendation to institutionalize imagination. It is easy to believe that using imagination to come up with scenarios can contribute more to the problem than to the solution, because unbridled imagination can produce a limitless supply of scenarios which exploit the vulnerabilities in countless targets. There is no end to the number of potential scenarios. Many of them seem credible, yet the nation's entire gross domestic product would not be sufficient to eliminate all of them from the realm of possibility. How is it possible to reconcile the tension between failure of imagination at

[39] *The 9/11 Commission Report*, 346.

one extreme, and the paralysis created by too much imagination at the other extreme? Clearly, what is needed is not unbridled imagination, but educated imagination.

Once again, collaboration provides the means to deal with the abundant "fruits" of imagination. Intelligence analysts might not be organizationally embedded into the offices of CIP or Vulnerability Assessment analysts, but the two groups should be so tightly integrated in practice that they each benefit from frequent and dynamic collaboration with each other. As each begins to develop a deep understanding of the needs and capabilities of the other, they can begin to agree on which scenarios are most likely to occur, and which would have the highest consequences. Even if this collaboration does not result in eliminating multitudes of scenarios from the list of possibilities, it can at least provide a way to prioritize them so that intelligence collection and resources may be directed against the most likely scenarios.

The Department of Homeland Security (DHS) created an innovative approach to thinking about how surprise attacks might be launched. DHS formed a team called the Analytic Red Cell with the stated goal of "promoting imaginative thinking about threats, vulnerabilities, and countermeasures."[40] This group challenges prevailing views and assumptions and tries to "get inside" the mind of an adversary in an effort to anticipate adversary planning. Perhaps the most innovative aspect of the Analytic Red Cell Program is not its goals, but its use of collaboration as the central element to accomplish those goals. The core staff of federal and contractor employees is supplemented by "hundreds of experts, creative thinkers, and individuals from around the country and world, including academics, psychologists, scientists, novelists, screenwriters, military war-gamers, special operations forces, cyber experts, think tanks, and industry specialists."[41] Using individuals with such diverse backgrounds (and even nationalities) maximizes opportunities for "getting inside the adversary's mind" for the purpose of anticipating attack modes.

[40] From an undated DHS information sheet on the Analytic Red Cell Program.

[41] *Ibid.*

Naysayers might argue that exercises such as this would generate better novels than realistic attack scenarios. That might be true, but during this initial stage, it is important to get all ideas out in the open and begin to categorize them in various ways. There will be opportunities in later steps to prioritize the scenarios based upon an estimate of the probability of likelihood of each scenario or category. It is also important to realize that during this early phase of the planning process, it is not necessary to divulge potential vulnerability information to participants who do not have the appropriate security clearances.

4. Step 2: "Identify Telltale Indicators Connected to the Most Dangerous Possibilities"

The Department of Homeland Security has provided the homeland security community with a variety of capabilities-based planning tools, including the National Planning Scenarios, the Universal Task List and the Target Capabilities List. The National Planning Scenarios give parameters for a variety of natural and man-made disasters so that analysts will have a place to begin their preparedness planning. The Universal Task List (UTL) is a reference menu of tasks which public and private organizations must cooperatively achieve in order to address major events. The Target Capabilities List (TCL) describes the capabilities that will be needed to perform some of the most critical tasks in the UTL. As they deal with scenarios, tasks and capabilities to prepare for disasters, homeland security planners should realize that potential adversaries must go through a similar process in order to *create* a disaster. This fact is the basis for the second step in the 9/11 Commission's process, that of identifying telltale indicators connected to the most dangerous possibilities. In essence, this step is a matter of determining the adversary's UTL and TCL for each scenario. The 9/11 hijacker's need for training on how to fly large commercial airliners is an example of a target capability that, had it been identified soon enough, could have led to a greater opportunity to "connect the dots" of information that had already been gathered before the attacks occurred.

Looking for telltale indicators might mean using old sources of information in new ways. For example, one of the tasks that terrorists must perform well if they are to be successful is to maintain public support in their home countries. Public support is

needed to fund their operations and to minimize interference from law enforcement. This task (one element of the terrorist's UTL) depends, in turn, upon the terrorist's capabilities (from their TCL) for using the media to communicate their message. One of the telltale indicators that the intelligence community should monitor is the shift in rhetoric and metaphor used by the media in Islamic countries to shape public opinion about the United States, its allies, and their operations. George Lakoff describes how the use of metaphor was used by the White House to prepare the United States for the first Gulf War in 1991. Lakoff argues that even if the U.S. had not been so clear in stating its intentions over a period of many months, Saddam Hussein should have known an attack was coming because of the government's use of strong metaphorical language.[42] This technique might provide useful telltale indicators that terrorists are attempting to build support for new attacks.

As with all other parts of the planning process, "looking for telltale indicators" cannot be successfully accomplished in a vacuum. Analysts need a continuous stream of information on the latest tactics being used by terrorists. The data needs to be sufficiently detailed and unprocessed to allow an analysis of the trajectory of technological and tactical developments. If current collection and reporting methods do not include this level of detail, a field analyst in any agency should be allowed to present a case for asking the intelligence collectors to modify their collection, analysis and reporting of post-event data. If analysts are able to synthesize a postulated trajectory of enemy tactical development, this could be used to assess and adjust the protection of critical infrastructure elements, predict future developments, and possibly even generate new and better intelligence tasking to look for additional precursors.

Once again, collaboration is an essential element for success in this part of the process as well. In his testimony before the 9/11 Commission, the acting director of the Defense Intelligence Agency stated, "Information considered irrelevant noise by one set

[42] George Lakoff, "Metaphor and War: The Metaphor System Used to Justify War in the Gulf," speech delivered to Audience at Alumni House, January 30, 1990, University of California, Berkeley, Berkeley, CA, http://lists.village.virginia.edu/sixties/HTML_docs/Texts/Scholarly/Lakoff_Gulf_Metaphor_1.html. (accessed February 4, 2006).

of analysts may provide critical clues or reveal significant relationships when subjected to analytic scrutiny by another."[43] This is a strong argument both for collaboration and information sharing.

5. Step 3. "Where Feasible, Collect Intelligence on These Indicators"

The two previous steps provide the foundation for entry into the traditional intelligence cycle. That is, they create the ability to focus intelligence collection requests to generate actionable information, and to improve future collection requests. Returning to John Boyd's OODA Loop analogy, the CIP and intelligence analysts must be able to receive new and relevant information in a timely manner ("observe"), assess the meaning of this new information in collaboration with others ("orient"), and then decide what new information or action is needed to broaden the understanding of the adversary. If this OODA Loop process can be operated efficiently and in a timely fashion, the analyst teams have a much better chance of asking for the right "dots" and then connecting them in a way that allows for the most relevant use of protection resources and which maximizes the potential for disrupting attacks in the planning or early execution stages.

The 9/11 Commission described this stage in the process as getting the intelligence system "tuned to comprehend the potential significance" of the information it is collecting.[44] The Commission cited as negative examples the July 2001 FBI report about potential terrorist interest in aircraft training, and the August 2001 arrest of Zacarias Moussaoui after he behaved suspiciously in flight school. Since the national intelligence community had not collaborated to think of possible scenarios and generate lists of tasks and capabilities needed by the adversaries to accomplish the scenarios, the intelligence system had not been "tuned" to understand the significance of this information about strange behavior in flight schools.

The Defense Advanced Research Projects Agency (DARPA), tested a remarkable program that performed the first three steps of this planning protocol. DARPA's approach sounds somewhat like datamining, but with a fundamental difference. Datamining is an *unguided* scan of large amounts of data to find patterns that look

[43] Testimony of RADM Lowell E. Jacoby, 9/11 Commission hearings, "Information Sharing on Terrorism-Related Data." 1 October 2002. Available [online]: http://9-11congress.netfirms.com/Jacoby.html. (accessed February 5, 2006).

[44] *The 9/11 Commission Report*, 347.

suspicious. Because datamining's success depends upon having a huge quantity and diversity of information upon which to operate, privacy advocates have expressed concerns about the loss of civil liberties that datamining could cause. DARPA's approach on the other hand, used the first two steps of the 9/11 planning protocol to implement the third step. That is, the DARPA method resulted in a very *targeted* scan of databases to look for evidence that certain scenario-dependent tasks and capabilities were being pursued by would-be terrorists. Dr. Tony Tether, Director of DARPA, described this program to Congress in the following manner:

> Our approach starts with developing attack scenarios, which are used to find specific patterns that could indicate terrorist plans or planning. These scenarios would be based on expert knowledge from previous terrorist attacks, intelligence analysis, new information about terrorist techniques, and/or from wargames in which clever people imagine ways to attack the United States and its deployed forces. The basic approach does not rely on statistical analysis to discover unknown patterns for creating predictive models. Instead, we start with expert knowledge to create scenarios in support of intelligence analysis versus a data mining approach that scans databases for previously unknown correlations.
>
> The scenarios would then be reduced to a series of questions about which data would provide evidence that such attacks were being planned. We call these scenarios "models," and they are, essentially, hypotheses about terrorist plans. Our goal is to detect data that supports the hypotheses.[45]

DARPA's imaginative attempt to implement the 9/11 Commission's recommendations unfortunately was derailed by Congressional action after pressure from a vocal minority overruled the technical and privacy merits of the program. This Congressional action might very well have further solidified the institutional inertia that suppresses imagination in government bureaucracies and makes innovators either look outside government for employment or decide that the safest career path is to avoid being imaginative. Success in the task of preparedness might very well depend upon future Congressional encouragement of these kinds of innovative programs, rather than their elimination.

---

[45] Testimony by Dr. Tony Tether, Director, Defense Advanced Research Projects Agency, in *Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census held in Washington, D.C., May 6, 2003*, U.S. House of Representatives (Washington, D.C. , 2003).

6. Step 4. "Adopt Defenses to Deflect the Most Dangerous Possibilities or at Least Trigger an Earlier Warning"

This final step of the 9/11 Commission's recommendation occurs after the first three steps have successfully returned data which indicates that a particular method of attack is of concern. Danger, or risk, involves a mixture of threat, vulnerability, and consequences. Proper interpretation of these variables may be known only within the context of an integrated, collaborative environment. To try to accomplish this step in a vacuum is to invite poor prioritization, over-spending to defend against less urgent threats and under-spending to defend against more urgent ones.

C. HOW MUCH IS ENOUGH? – PART II

> Defenses cannot achieve perfect safety. They make targets harder to attack successfully, and they deter attacks by making capture more likely. Just increasing the attacker's odds of failure may make the difference between a plan attempted, or a plan discarded. The enemy also may have to develop more elaborate plans, thereby increasing the danger of exposure or defeat.[46]

The first step in the 9/11 Commission's planning protocol is to generate potential attack scenarios. Scenario planning teams should seek law enforcement and intelligence community input whenever possible. For each scenario, the planning team should estimate the number of terrorist cells, and the size of each cell, that would be needed to accomplish the attack. Law enforcement personnel should be asked for their professional judgment as to the probability that the terrorist cell(s) would be detected by law enforcement or other means during any stage of planning, reconnaissance or preparation before the attack. Planners should ask themselves and their law enforcement counterparts how hardened a target would have to be to force the adversary into the realm of detectability by law enforcement. The kind of hardening that would increase the probability of detection before the attack consists of techniques or procedures that cause one or more of the following effects for the adversary:

- Increase the amount of surveillance needed to plan the attack
- Increase the amount of equipment needed to carry out the attack
- Increase the number of attackers needed to carry out the attack

[46] *The 9/11 Commission Report*, 383.

- Increase the amount of coordination needed to plan and carry out the attack
- Increase the amount of time the attackers need to carry out the attack
- Increase the complexity of the attack so as to decrease the probability of its success
- Decrease the likelihood that an attack would even be attempted, because of the low probability the attacker would achieve the desired consequences

Fixed spacing on bullets - .5 from left margin and 6 pt after

As a hypothetical example, suppose that one attack scenario against an unhardened target would require a cell of five terrorists to conduct the planning and operations. Law enforcement experts might determine that they would detect a cell of five terrorists planning and conducting these operations with a probability of only 15%. But if the target could be hardened to a certain degree, analysts might estimate that it would now require ten terrorists to accomplish the same attack, and that they would have to purchase and learn how to use some equipment that is relatively uncommon. Law enforcement experts might decide their probability of detecting this attack in the planning or early execution stages would jump to 60%. In such a case, the protection planners might determine that this amount of hardening would be sufficient according to their risk management approach. A collaborative approach such as this not only helps design cost-effective hardening measures, it helps "tune the system" to detect preparations in advance by getting law enforcement officials involved in the planning stages.

D. WARNING

Our nation has had too many opportunities to witness the damage that can be caused by a traitorous spy, someone the security community refers to as an "insider." The damage caused by an insider can be great, even when information is heavily compartmented and very few people have access to the "big picture." The potential Achilles' Heel of enhanced information sharing and collaboration is the malevolent insider. As we move toward an environment where much more sensitive strategic and tactical information is distributed to thousands of people in many parts of the government, this increases the likelihood of an insider getting the information and it dramatically increases the amount of damage that one malevolent insider can cause.

Despite their ponderous inertia, our governmental institutions are moving inexorably into a more networked, collaborative era, and our insider protection and detection technologies must not be allowed to fall behind. To proceed in an unbalanced fashion toward a more networked, but inadequately protected, environment is to forfeit to every potential adversary the ultimate asymmetric tool with which to destroy us – our most sensitive critical infrastructure protection information. The very information that has the potential to protect us can also serve as the ultimate weapon for our adversaries.

VII. APPLICATION TO THE DEPARTMENT OF ENERGY[47]

> Furthermore, we made the terrible mistake ... of forgetting that a fine deterrent can make a superb target.[48]

A. THE MISSION OF THE DEPARTMENT OF ENERGY

The United States Department of Energy (DOE) is charged with building and maintaining the nation's stockpile of nuclear weapons.[49] The DOE's protection planning process for its nuclear facilities has evolved over many years and is neither derived from nor driven by homeland security policy. Instead, the policy requirements for the protection of these facilities is found in the Atomic Energy Act, the Code of Federal Regulations and internal DOE directives. Even so, the principles from the previous chapters are so broadly applicable that they will be used to show areas where DOE could improve its processes.

B. UNIQUE FACILITIES – "WEAPONS IN PLACE"

The DOE's nuclear weapons work is carried out at several government-owned, contractor-operated facilities, as shown in Figure 3. These facilities are critical to national security, not only because of the vital role they play in maintaining our nuclear deterrence capability, but also because the information and materials they protect would be so dangerous if they were to get into the wrong hands. Homeland Security secretary Michael Chertoff's description of certain facilities as "weapons in place" would certainly apply to DOE's nuclear facilities.[50] "Weapons in place" is a phrase Mr. Chertoff used to

---

[47] The author uses several lengthy quotations from official, open source, government statements in this chapter as a means of ensuring that no classified or sensitive information is inadvertently included.

[48] Wohlstetter, *Pearl Harbor*, viii.

[49] DOE accomplishes this through the semi-autonomous National Nuclear Security Administration whose Administrator reports to the Secretary of Energy. Unless there is a need to distinguish between the roles of the two organizations in this thesis, the two will be referred to collectively as DOE.

[50] Testimony of Hon. Michael Chertoff, Secretary of Homeland Security. Senate, Homeland Security and Governmental Affairs Committee. 14 July 2005. Available [online]: http://www.dhs.gov/dhspublic/display?content=4631/ (accessed February 3, 2006).

describe facilities in which a terrorist could find enough chemicals, biological agents or nuclear materials to make a weapon of mass destruction without having to bring those materials from the outside.

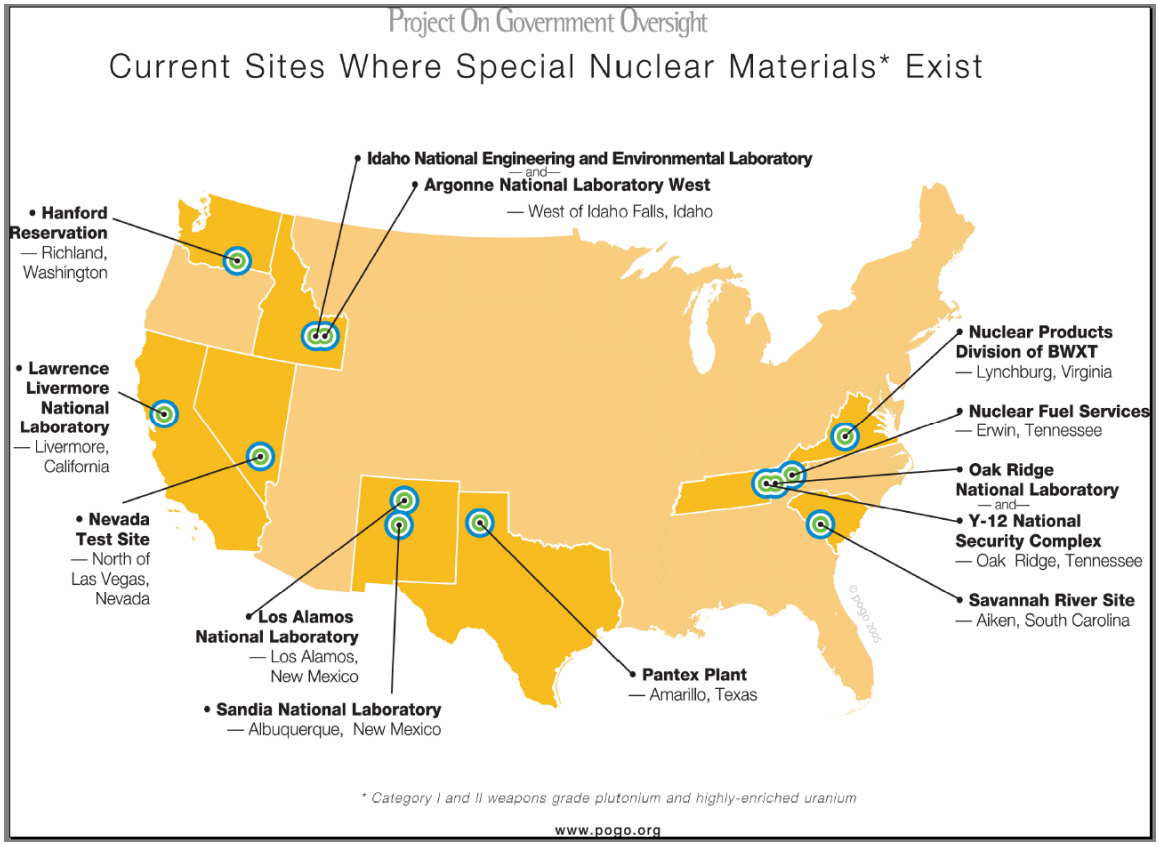

Figure 3. DOE Sites Containing Special Nuclear Materials
Source: http://www.pogo.org/m/hsp/2005nuclear/NukeX.pdf

The Government Accountability Office acknowledged the unique nature of these facilities when they wrote, “DOE has long recognized that a successful terrorist attack on a site containing the material used in nuclear weapons—called special nuclear material—could have devastating consequences for the site and its surrounding communities. This is particularly true at sites that contain Category I special nuclear material, which consists of specified quantities of plutonium and highly enriched uranium in the form of assembled nuclear weapons and test devices, major nuclear components, and other high-

grade materials such as solutions and oxides."[51] A successful attack against one of these facilities could damage the ability to maintain the necessary level of our nation's nuclear deterrence, cause serious health and environmental consequences within and beyond the boundary of the site, and provide materials terrorists would need to make multiple weapons of mass destruction which could then be used at multiple locations. These unique characteristics provide the justification for hardening these facilities to an extraordinarily high degree.

C. PLANNING FOR DOE'S CRITICAL INFRASTRUCTURE PROTECTION

DOE's security analysis, planning and protection system could be diagrammed in many ways depending upon which element(s) are being emphasized. Figure 4 puts the vulnerability assessment (VA) analyst at the center of the diagram.

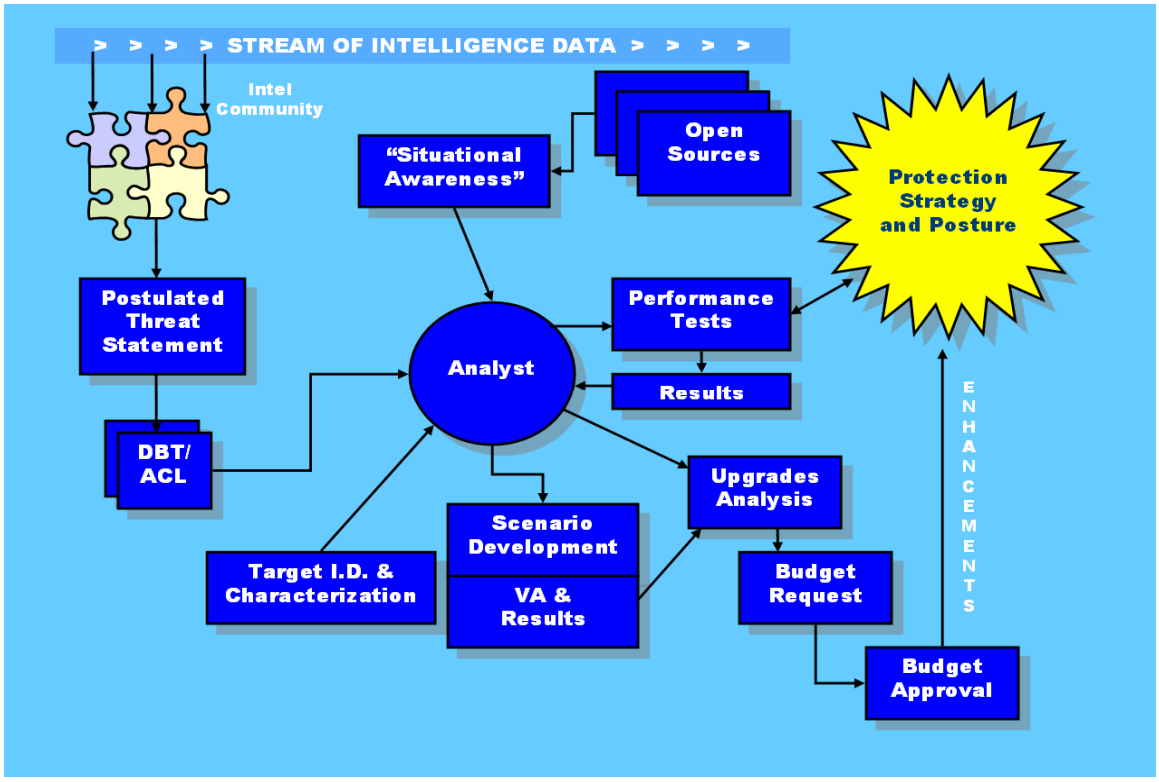

Figure 4. DOE Protection Planning and Testing Diagram

[51] Testimony of Robin M. Nazzaro, U.S. Congress, House, Committee on Government Reform. "Several Issues Could Impede the Ability of DOE's Office of Energy, Science and Environment to Meet the May 2003 Design Basis Threat." 22 June 2004.

The term "analyst" in this case may refer to a team of analysts or to anyone who is involved in the planning and analysis process. These VA analysts are DOE's equivalent to Critical Infrastructure Protection (CIP) analysts in the field of homeland security. The Protection Strategy and Posture, shown in the upper right corner of the diagram, is the output of the entire process and is where planning meets reality. The Protection Strategy and Posture is the reason for the existence of the entire planning system and includes everything from the number of protective forces and their weaponry, deployment, tactics and training, to the hardware, software, processes and personnel who protect the valuable information and assets at these facilities. Figure 4 reveals a variety of "inputs" from which the analyst must draw, as well as the "outputs," or work products the analyst must produce. The "Target Identification and Characterization" block represents all of the valuable assets at the facility that might be potential terrorist targets. The "Situational Awareness" block represents the analysts' existing knowledge, based upon training, education and life experiences, as well as sources of fresh information, all of which help the analyst orient properly to the threat environment. Most of the VA analyst's new situational awareness information comes from open sources, although there is no supplier of such information that develops information products specifically with the needs of VA analysts in mind. At very infrequent intervals, typically two to four times per year, classified intelligence briefings are presented by DOE Headquarters to its field sites via secure teleconference. These briefings, although classified, are heavily sanitized to remove any information about sources and methods, and seem to be designed to help the diverse audience get an overall sense of what is happening in the threat environment rather than to provide details on past terrorist attacks or details about the terrorists' plans as described in captured materials or through interviews with detainees.

Of particular importance for the purpose of this thesis is the left hand side of Figure 4. The agencies which make up the Intelligence Community, shown at the top, draw from the available stream of intelligence information and produce databases of information as well as finished reports. One such report is the Defense Intelligence Agency's classified *Postulated Threat to U.S. Nuclear Weapons Facilities and Other Selected Strategic Facilities*, usually referred to as the Postulated Threat Statement. The Postulated Threat Statement provides threat information about postulated adversary team

sizes, characteristics, capabilities and applicability to national security assets. The Postulated Threat Statement is based on intelligence information detailing actual terrorist attacks and the equipment and tactics utilized in the attacks, expert judgments regarding stated terrorist intentions and the ability of the terrorist to execute the stated objectives, and postulated capabilities based on the latest knowledge concerning terrorist activities.[52]

Department of Energy headquarters uses the Postulated Threat Statement to develop two DOE-specific documents: the Design Basis Threat (DBT) and the Adversaries Capabilities List (ACL). These two classified documents define the numbers and types of adversaries against which the site must be prepared to defend, as well as capabilities such as training and equipment which those adversaries might be expected to have and use.[53] (CIP analysts might want to think of the DBT and ACL as being roughly equivalent to an *adversary's* version of a Target Capabilities List.) As mentioned earlier, the protection posture consists of the security forces, procedures and systems which are used protect against a wide array of possible attacks, including cyber attacks and malevolent "insiders." The DBT and ACL are derived from intelligence information, but their purpose is not to provide intelligence information. Rather, they serve as the performance specification against which each DOE facility must design and test its protection strategy and posture. The post-9/11 DBTs have set a very challenging standard of protection, or hardening, for all DOE nuclear facilities, and the amount of hardening required is graded according to the particular types and quantities of materials at a given site. "The 2003 DBT assumes that terrorist groups are the following: well armed and equipped; trained in paramilitary and guerrilla warfare skills and small unit tactics; highly motivated; willing to kill, risk death, or commit suicide; and capable of attacking without warning. Furthermore, according to the 2003 DBT, terrorists might attack a DOE facility for a variety of goals, including the theft of a nuclear weapon, nuclear test device, or special nuclear material; radiological, chemical, or biological

[52] Testimony of Joseph S. Mahaley, US Congress, House, Committee on Government Reform. 24 June 2003. Available [online]: http://www.energy.gov/print/2343.htm. (accessed January 16, 2006).

[53] Testimony of Gene Aloise, US Congress, House, Committee on Government Reform. "Actions Needed by DOE to Improve Security of Weapons-Grade Nuclear Material at its Energy, Science and Environment Sites." 26 July 2005.

sabotage; and the on-site detonation of a nuclear weapon, nuclear test device, or special nuclear material that results in a significant nuclear yield. DOE refers to such a detonation as an improvised nuclear device."[54]

Prior to the attacks of 9/11, the most recently published Postulated Threat Statement was issued in 1994 and was intended to be used for ten years.[55] After the 9/11 attacks, updates to the Postulated Threat Statement and the DBT continued in parallel as much as possible. The new Postulated Threat Statement was issued in January, 2003 and the DBT followed on May 20, 2003. This planning tempo is analogous to that of the DoD's during the Cold War, when the presumed adversaries were nations whose planning tempos were roughly equivalent. DOE has hastened the pace of planning and was able to issue the two most recent DBT updates within a period of 19 months. Even so, due to the slow federal budget process and the number of years it takes to get physical upgrades approved, designed and constructed, much work has to be done within DOE just to comply with the DBT that was issued in 2003 in reaction to the attacks of 9/11.

Once a site's protection posture is defined and put into place, DOE maintains an ongoing process, shown in Figure 4, of developing attack scenarios, designing performance tests, analyzing potential upgrades and justifying additional resources to support those upgrades.

D. INFORMATION CONTAINMENT

That same figure reveals, however, that the daily stream of intelligence information does not make its way to the VA analyst in the field. The analyst might have some very general unclassified open source material with which to enhance his or her situational awareness and provide new data to spark imaginative scenario development, but there is no formal mechanism which requires that all VA analysts be provided the most highly classified and up-to-date intelligence information. Some might argue that such access is not necessary since the DBT was derived from intelligence information.

[54] Testimony of Robin M. Nazzaro, U.S. Congress, House, Committee on Government Reform. "Several Issues Could Impede the Ability of DOE's Office of Energy, Science and Environment to Meet the May 2003 Design Basis Threat." 22 June 2004.

[55] Testimony of Joseph S. Mahaley, US Congress, House, Committee on Government Reform. 24 June 2003. Available [online]: http://www.energy.gov/print/2343.htm. (accessed January 16, 2006).

But the DBT itself is two steps removed from the actual intelligence information, and is, in fact, a design specification rather than an intelligence report. Furthermore, its update frequency is measured in years rather than days – perhaps appropriate given its purpose as a design specification – but the DBT is insufficient to meet analysts' needs in today's threat environment. The significance of this information gap is apparent when one realizes that a similar isolation of analysts from pertinent intelligence information resulted in a tragic failure of analysis and action within the Federal Aviation Administration (FAA) before 9/11, as described in Chapter IV.

E. COLLABORATION

The limitation mentioned above is only one symptom of a larger issue, and that is the lack of representation of field perspective in the processes of intelligence collection and distribution as well as in the preparation of the Postulated Threat Statement and the DBT/ACL. Figure 4 reveals that the overall flow of information that is derived from classified intelligence is for the most part, unidirectional. There is no formal structure to ensure that field analysts provide feedback to, or request information from, the intelligence community. This isolation means that there is no structured mechanism to promote robust collaboration between DOE VA analysts and intelligence analysts, and therefore, no way to involve the VA analysts in the intelligence cycle recommended by the 9/11 Commission and described in Chapter VI. The purpose of establishing this relationship is not to fulfill any optimistic notion that it would lead to advance warning of the date and time of an impending attack. The characterization of the low-signature threat in Chapter 2 should be sufficient to inform us that the advance notice of an attack would be extremely unlikely and should not be counted upon. Instead, the interaction between the VA and intelligence analysts would serve the following two-fold purpose:

- Establish a collaborative environment for scenario development and intelligence tasking to enable all parties to gain a better understanding of the intelligence collection needs, possibilities and limitations.
- Provide a steady flow of information related to the terrorist tactics being used throughout the world, but especially in the dynamic environments of Afghanistan and Iraq, where the terrorists are constantly refining their operational and tactical techniques to overcome new counter-insurgency initiatives of coalition forces. Such detailed information might very well

contain subtleties that could have significance only to a field VA analyst who could immediately put the information to use.

A simple modification to the previous diagram shows the recommended connections that would cultivate the benefits of information sharing and collaboration. The changes indicated by the red arrows in Figure 5 would allow the VA analysts in the field to get relatively unfiltered information about current and potential terrorist tactics at the same time that headquarters receives that information. This modification would move toward a more networked environment with better timeliness of information.

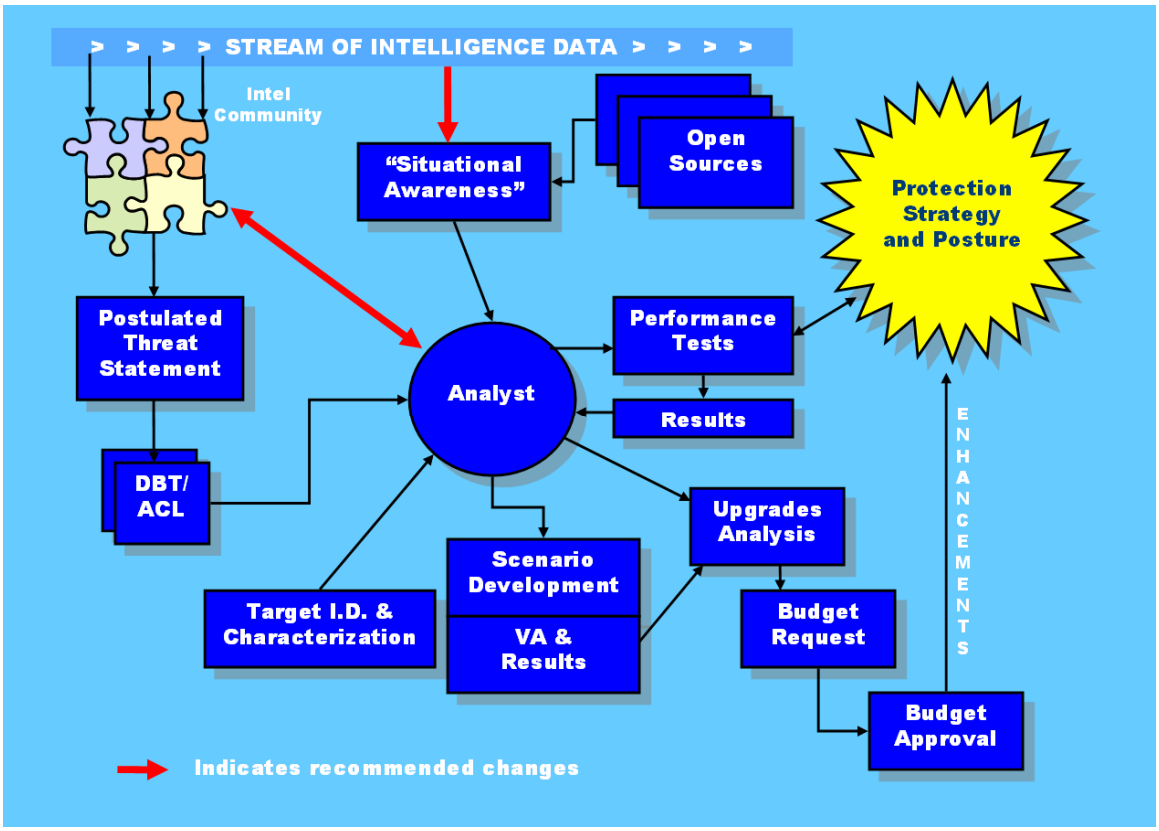

Figure 5. DOE Planning Diagram Showing Recommended Changes

F. INCREASING THREAT

One additional reason that such interaction between the VA and intelligence analysts is crucial is that post-9/11 versions of the DBT "significantly increased" the size of the adversary force that must be successfully countered.[56] The significance of this fact is that the number and complexity of possible attack scenarios, and therefore the challenge of defending against those scenarios, increases exponentially as the adversary numbers and capabilities increase. A strong, collaborative atmosphere is therefore essential to generate and assess the myriad new attack scenarios that would not have been possible with the smaller attacking force described in previous DBTs.

Before 9/11, when the number of adversaries against which DOE sites had to defend was significantly lower and the complexity of potential attack scenarios was less challenging, it is quite possible that the infrequently updated Postulated Threat Statements, DBTs and ACLs provided adequate information for the VA analysts. With the dramatic post-9/11 increases in both the DBT and ACL however, the VA analysts need all the information they can get to help them think of new attack scenarios. The purpose is not to exceed the bounds set by the DBT and ACL, but to be able to think of the vastly greater number of challenging scenarios that fall within DBT parameters, and to design protection measures that would defend against many, rather than just one or a few, attack modes.

Security managers at DOE headquarters would be justifiably concerned at this suggestion, thinking that the analyst's imaginations might run wild with too much new information. But the interaction between the VA and intelligence analysts would provide strong justification for ensuring that "wild" scenarios were documented and removed from further consideration, thereby eliminating the possibility of spending resources unwisely. The synergy that could be developed between the two groups of analysts could conceivably help identify relatively inexpensive modifications to current procedures or structures (analogous to hardened cockpit doors) that would help reduce vulnerabilities to scenarios that might not have been thought of otherwise.

---

[56] Testimony of Glenn S. Podonsky, US Congress, House, Subcommittee on National Security, Emerging Threats, and International Relations. "Readiness of Department of Energy Protective Forces." 26 July 2005.

Finally, intelligence reports can contain information that might never find its way into a design specification such as the DBT/ACL, but which would be very important for a field analyst to know. Referring back to Colonel Boyd's OODA diagram in Chapter 4, each analyst's orientation mechanism causes them to see information in unique ways. The intelligence collector outside of DOE, the DOE intelligence analyst and the DOE field analyst each might gain something different from the same intelligence report. An element of data that might seem insignificant to one could be of tremendous significance to another. A subtle change in terrorist attack tactics in Iraq, for example, might pass without notice in the mind of an intelligence collector, but could have serious implications to a field analyst because of a particular facility feature or vulnerability that only that analyst would know about.

G. HOW MUCH IS ENOUGH IN THE DEPARTMENT OF ENERGY?

The DOE nuclear field sites do not participate in the second and third steps of the 9/11 protocol; that is, they do not generate adversary "target capabilities lists" based upon the scenarios they have developed, nor do they seek intelligence collection against those lists. There is no mechanism in place to allow or cause this collaboration to occur.[57] It is useful to consider whether this apparent deficiency really matters. After all, if any scenario falls within the bounds of the DBT/ACL, then the sites are required to be prepared to defend themselves against that scenario. It would be pointless, one could argue, to ask the intelligence community to gather information on potential attack preparations if the sites are already supposed to be able to defend against that scenario. The problem with this argument is that it leaves site managers without a collaboration-enhanced means of prioritizing their own security upgrades, and it leaves headquarters managers in an even more difficult situation since they must prioritize all the security upgrade requests from multiple sites across the entire DOE complex. A collaborative effort between the VA and intelligence analysts is needed to help sort through the scenarios and determine which ones are most likely to occur based upon current information. The second problem with this situation is the absence of the second step of

[57] Some components of this security-intelligence interaction might be occurring internally at DOE headquarters, but it is not apparent to the field sites, nor is field site perspective part of the discussion.

the 9/11 Commission's recommended approach. This failure to seek information about potential terrorist preparations for attack deprives the intelligence community of a good source of potential tasking ideas that could "tune the system" to discover of an attack during the planning and preparation stages. Furthermore, site analysts might help generate ideas for new intelligence collection capabilities that do not yet exist, but which could provide valuable information to enhance preparedness. Finally, as adversary numbers and capabilities have increased in the DBTs and ACLs since 9/11, and the number of challenging scenarios has risen exponentially, it is difficult or impossible to know whether the most challenging ones have been thought of yet. The sites then find themselves at the mercy of inspectors and review teams who test the site's defenses using their own favorite scenarios. But there is no reason to believe that the pet scenarios of a review team are any more or less likely to occur than the site's own scenarios.

H. A PROPOSED MECHANISM TO START COLLABORATION

This vast multiplication of potential scenarios is just one more reason that it is essential for the analysts to get unfiltered data on a regular basis. This could be done by requiring each analyst to spend hours in front of a computer screen each week, looking through hundreds of intelligence reports. Since VA analysis time is in short supply these days, this would not be an effective use of resources. It would be better to have regular collaborative meetings between intelligence and VA analysts. As those two groups begin to understand the information needs and capabilities of each other, the intelligence office at DOE headquarters would be able to produce or acquire intelligence products that would be tailored to the needs of the field analysts. Even so, the analysts should always have on-demand "pull" access to all information that might be of use so they can look for new technical, tactical and political developments that could impact their ability to defend against the terrorist threat.

One mechanism that might fulfill this purpose would be the existing Vulnerability Assessment Technical Working Group (VATWG), sponsored by DOE headquarters. The VATWG consists of a subset of the site VA analysts who meet once or twice each year to discuss the VA process, usually in an unclassified meeting room. These meetings could be turned into collaborative events with intelligence analysts and others who should be

involved. All VATWG participants should be cleared for SCI information, and the meeting should be held in an environment where classified information could be discussed. As discussed in the previous chapter, however, this collaboration must be carefully planned. Simply mandating collaboration, without first engendering the vision for it, is likely to result in a cynical and detrimental reaction.

I. SUMMARY

The Department of Energy has, over many years, created a profoundly effective approach for hardening its sites against terrorist attacks. As the threat becomes more challenging however, DOE must continue to look for opportunities to increase collaboration among all who could contribute to the security planning process, and should seek to develop a "common operating picture" among all analysts and managers. Information sharing should be dramatically escalated and focused on the needs of the site analysts. A highly collaborative group should be used to help prioritize scenarios and proposed upgrades at each site and across the DOE complex. This would strengthen the basis for DOE's security budget requests and bring more focus to the vulnerability assessment and intelligence collection processes in support of the nuclear weapons complex.

VIII. CONCLUSION

> If the study of Pearl Harbor has anything to offer for the future, it is this: We have to accept the fact of uncertainty and learn to live with it. No magic, in code or otherwise, will provide certainty. Our plans must work without it.[58]

Our adversaries have many ways to continuously probe our open society with relative safety and anonymity as they gain a better understanding about the operation of our critical infrastructure and protection measures. We must be just as aggressive in our probing to find out what they are learning, how they are applying their knowledge to overcome our defenses, and what they are thinking about doing to harm us in the future.

Critical Infrastructure Protection analysts must carefully analyze their own connectedness to the sources of information and collaboration that will maximize their situational awareness and "orientation." This should include sources who can help them identify and challenge internal biases that limit their ability to properly interpret new information. Managers who oversee the work of CIP analysts must do the same, and ensure their analysts are not too inwardly focused.

All CIP analysts must put the 9/11 Commission's targeted intelligence collection process to work, even if it is on a small scale. The Department of Homeland Security has published a set of national planning scenarios, but it is up to the CIP analyst to use a variety of sources to help them come up with specific attack modes that fit in with those planning scenarios. Only then can the analysts begin to develop a conceptual version of a terrorist's "target capabilities list" and then request collection of intelligence against those lists, where possible. Collaboration with intelligence personnel in this process can help prioritize the risks and show where resources are most urgently needed to ensure preparedness.

[58] Wohlstetter, *Pearl Harbor*, 401.

Analysts must seek innovative ways to harden and monitor our nation's critical infrastructure in order to raise the risk of exposure for the planners of terrorism. Analysts must also keep their law enforcement contacts informed about possible scenarios so they might be better attuned to the significance of new information they find during their law enforcement activities.

Finally, analysts and their managers should take to heart the 9/11 Commission's criticism that the greatest failure which permitted the events of September 11, 2001 to occur was the failure of imagination. An organization cannot be expected to create imagination where it does not exist nor enforce its effective use. But any organization can at least institutionalize the process of fostering a collaborative environment and providing a rich and steady stream of information with which to cultivate imagination. Measures such as the ones presented in this thesis cost very little to implement and can increase synergy and camaraderie within the intelligence and CIP analyst communities, enhance the analysts' situational awareness, improve their ability to develop imaginative yet realistic scenarios (including a greater ability to prioritize scenarios and eliminate unrealistic ones), improve the kinds of performance tests they use to measure the effectiveness of their protection strategies, and improve their ability to justify protection upgrades.

This thesis ends as it began – with a reminder from the 9/11 Commission that a rededication to preparedness is perhaps the best way to honor the memories of those we lost on September 11, 2001. We cannot succeed in the mission of preparedness by mandating collaboration and information sharing. Instead, we must make every effort to ignite within others the vision of what can be gained through effective co-laboring and information sharing. Only then will we see the formation of a cadre of impassioned preparedness planners who will not rest until they see that vision become a reality through the constant improvement of our processes, our collaboration and ourselves. May we never grow weary in this great endeavor.

LIST OF REFERENCES

Arquila, John, David Ronfeldt, and Michele Zanini. "Networks, Netwar and Information-Age Terrorism." In *Countering the New Terrorism*, ed. RAND National Defense Research Institute, 39-84. Washington, D.C.: RAND, 1999.

Chertoff, Michael. "Testimony of Secretary of Homeland Security Michael Chertoff." In *Homeland Security and Governmental Affairs Committee held in Washington, D.C., July 14, 2005*, U.S. Senate. Washington, D.C. Available [online]: http://www.dhs.gov/dhspublic/display?content=4631/ (accessed February 3, 2006).

The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction. *Report to the President of the United States*. Washington, D.C.: , 2005.

Coram, Robert. *Boyd: The Fighter Pilot Who Changed the Art of War*. Boston: Little, Brown & Company, 2002.

Crumpton, Henry A. "U.S. Counterterrorism Strategy Update." In *House International Relations Committee Subcommittee on International Terrorism and Nonproliferation held in Washington, D.C., October 27, 2005*, U.S. House of Representatives. Washington, D.C.:, 2005. http://usinfo.state.gov/is/Archive/2005/Oct/28-580190.html. (accessed January 26, 2006).

Davis, Paul K. *Analytic Architecture for Capabilities-Based Planning, Mission-System Analysis and Transformation*. Washington, D.C.: RAND National Defense Research Institute, 2002.

Department of Homeland Security. *Final Draft of National Preparedness Goal*. Washington, D.C.: Department of Homeland Security, December, 2005.

Henry, Ryan. "Defense Transformation and the 2005 Quadrennial Defense Review." *Parameters* 35, no. 4 (Winter 2005-06): 5-15.

Inge, Joseph R. and Eric A. Findley. "North American Defense and Security after 9/11." *JFQ*, no. 40 (First quarter 2006): 23-28.

Kam, Ephraim. *Surprise Attack: The Victim's Perspective*. Cambridge, MA: Harvard University Press, 1988.

Kendall, Jeffrey B. *Capabilities-Based Planning: The Myth*. : National Defense University, National War College, 2002.

Lakoff, George. "Metaphor and War: The Metaphor System Used to Justify War in the Gulf." Speech delivered to Audience at Alumni House, January 30, 1990. University of California, Berkeley, Berkeley, CA. http://lists.village.virginia.edu/sixties/HTML_docs/Texts/Scholarly/Lakoff_Gulf_Metaphor_1.html. (accessed February 4, 2006).

Lewis, Ted G. "Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation." (Unpublished manuscript, Naval Postgraduate School, Monterey, California. 2004)

Lowenthal, Mark M. *Intelligence: From Secrets to Policy*. Washington, D.C.: CQ Press, 2003.

Mahaley, Joseph S. "Subcommittee on National Security, Emerging Threats, and International Relations." Committee on Government Reform, Washington, D.C., June 24, 2003, U.S. House of Representatives. Washington, D.C. Available [online]: http://www.energy.gov/print/2343.htm. (accessed January 16, 2006).

Miller, Mark E. *The Integration of Operations and Intelligence: Getting Information to the Warfighter*. Air Command and Staff College, Research Department, 1997. , AU/ACSC/0362/97-03.

National Commission on Terrorist Attacks Upon the United States. *The 9/11 Commission Report*. New York: W. W. Norton & Company, 2004.

Nazzaro, Robin M. "Several Issues Could Impede the Ability of DOE's Office of Energy, Science and Environment to Meet the May 2003 Design Basis Threat." Committee on Government Reform. June 22, 2004. U.S. House of Representatives. Washington, D.C.: GAO, 2004.

Office of the Inspector General, United States Department of Energy. *The National Nuclear Security Administration's Implementation of the 2003 Design Basis Threat*. Washington, D.C.: DOE, 2005.

Pelfrey, William V. "The Cycle of Preparedness: Establishing a Framework to Prepare for Terrorist Threats." *Journal of Homeland Security and Emergency Management* 2, no. 5 (2005): 5:1-21.

Podonsky, Glenn S. Subcommittee on National Security, Emerging Threats, and International Relations. "Readiness of Department of Energy Protective Forces" July 26, 2005, U.S. House of Representatives. Washington, D.C.:, 2005.

Surowiecki, James. *The Wisdom of Crowds*. New York: Anchor Books, 2005.

Tether, Tony. "Testimony by Dr. Tony Tether, Director, Defense Advanced Research Projects Agency." Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, May 6, 2003, U.S. House of Representatives. Washington, D.C.: , 2003.

U.S. President. *Executive Order.* "Further Strengthening the Sharing of Terrorism Information to Protect Americans." (27 October 2005) Available [online]: http://www.whitehouse.gov/news/releases/2005/10/print/20051025-5.html. (accessed February 3, 2006).

Wohlstetter, Roberta. *Pearl Harbor: Warning and Decision.* Stanford, CA: Stanford University Press, 1962.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Paul Stockton, Director
   Center for Homeland Defense and Security
   Naval Postgraduate School
   Monterey, California

4. Gary D. Wisdom
   United States Department of Energy
   Amarillo, Texas

5. Daniel E. Glenn
   United States Department of Energy
   Amarillo, Texas